Хмельницький національний університет
Факультет інформаційних технологіїй
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Підсистема забезпечення безпеки IP -телефонії в корпоративній мережі
Назва теми

КвРКІ 210104.21.01.31 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»
Назва

Виконав: студент IV курсу, група КІ2–21–1 _____ Даниїл БРИНДІКОВ
Підпис Ініціали, прізвище

Керівник _____ Світлана САЧЕНКО
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис Ініціали, прізвище

«16» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

"10" 04 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Даниїлу БРИНДІКОВУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Підсистема забезпечення безпеки IP -телефонії в корпоративній мережі

Керівник проекту (роботи) Світлана САЧЕНКО., к.е.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. №23

2. Строк подання студентом проекту (роботи) на кафедру 20.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Теоретичні основи забезпечення безпеки в IP-телефонії

Система забезпечення безпеки використання IP-телефонії

Реалізація та тестування системи безпеки для IP-телефонії в корпоративній мережі на базі Asterisk

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Демонстрація зареєстрованого софтфона

Схема роботи Fail2Ban

Система IP-телефонії на прикладі Asterisk

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «_11_»_____01_____2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2025	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконан
3	Робота над розділом 1 аналіз відомих моделей, методів за темою; постановка задачі	01.03.2025	виконан
4	Робота над розділом 2 - розробка моделей для вирішення поставленої задачі	01.04.2025	виконан
5	Робота над розділом 3- розробка методів для вирішення поставленої задачі	30.04.2025	виконан
6	Оформлення пояснювальної записки згідно вимог	20.05.2025	виконан
7	Попередній захист ВКР	30.05.2025	виконан
8	Захист ВКР на засіданні ЕК	Червень 2025 року	

Студент Підпис Даниїл БРИНДІКОВ (Ініціали, прізвище)

Керівник проекту (роботи) Підпис Світлана САЧЕНКО (Ініціали, прізвище)

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ. 210104.21.01.31ПЗ	Пояснювальна записка	56		
			Графічні матеріали			
2		КвРКІ. 210104.21.01.31Е8	Демонстрація	1		
			зареєстрованого софтфона			
3		КвРКІ. 210104.21.01.31Е2	Демонстрація	1		
			роботи Fail2Ban			
4		КвРКІ. 210104.21.01.31Е4	Система IP-телефонії	1		
			на прикладі Asterisk			

Зм	Арк	№ докум	Підпис	Дата	КвРКІ. 210104.21.01.31ПЗ		
Розробив		Бриндіков Д.Ю.			Відомість проєкту	Літера	Аркуш / Аркушів
Перевір.		Савченко С.І.				У	1 / 1
Н. контр.		Кисіль Т.М.				ХНУ, КІ2-21-1	
Затв.		Павлова О.О.					

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Підсистема забезпечення безпеки IP - телефонії в корпоративній мережі».

Автор роботи: *Даниїл БРИНДІКОВ*.

Керівник роботи: *Світлана САЧЕНКО*.

Пояснювальна записка: *58 с.*, *5 рис.*, *3 дод.*, *40 джерел*.

ПІДСИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ.

Розвиток сучасних телекомунікаційних технологій, зокрема IP-телефонії, відкриває нові можливості для підвищення ефективності комунікацій у межах корпоративних мереж. Водночас зростає актуальність питань безпеки, пов'язаних із передачею голосових даних через відкриті мережі, що вимагає впровадження спеціалізованих технічних рішень для захисту інформації.

Підсистема забезпечення безпеки IP-телефонії в корпоративній мережі є важливим компонентом загальної інформаційної безпеки організації. Вона дозволяє виявляти і запобігати загрозам, пов'язаним із несанкціонованим доступом, перехопленням голосових даних, атакою типу «людина посередині» (MITM) та іншими потенційними ризиками.

Сучасні технології, зокрема використання протоколів шифрування (наприклад, SRTP, TLS), а також систем автентифікації та контролю доступу, забезпечують надійний рівень захисту. Крім того, застосування міжмережевих екранів, систем виявлення вторгнень (IDS/IPS) та аналізу трафіку дозволяє будувати гнучку і масштабовану архітектуру захисту IP-телефонії.

Такий підхід є принципово важливим кроком у розвитку безпечних корпоративних комунікацій, демонструючи значний потенціал сучасних інформаційно-комунікаційних технологій у створенні надійного та захищеного середовища для передачі голосових даних.

Підпис студента _____ Дата 6.06.2025

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

VoIP - передача голосових дзвінків через мережу

QoS - пріоритетність обробробки голосових дзвінків

SIP - установчий протокол

RTP - протокол транспортування голосових пакетів в реальному часі

SRTP - протокол шифрування

ВСТУП

У сучасному світі швидко розвиваються інформаційні технології, що значною мірою змінюють спосіб ведення бізнесу та організації комунікацій у корпоративних середовищах. Одним із основних елементів, що визначають ефективність внутрішніх і зовнішніх комунікацій підприємств, є системи IPтелефонії. Вони дозволяють забезпечити зручність і ефективність обміну голосовою інформацією через інтернет-протоколи, значно знижуючи витрати на традиційні телефонні системи та відкриваючи нові можливості для розвитку компаній у цифрову епоху.

Незважаючи на численні переваги, які пропонує технологія IP-телефонії, її впровадження та використання супроводжується рядом безпекових ризиків. Це обумовлено тим, що голосовий трафік, який передається через Інтернет, може бути підданий різним видам атак, таким як перехоплення даних, атаки типу "відмова в обслуговуванні" (DoS), спроби несанкціонованого доступу до мережі та інші загрози. Без належного захисту корпоративні мережі стають уразливими перед кіберзлочинцями, що може призвести до серйозних фінансових та репутаційних втрат для компанії.

Проблема забезпечення безпеки IP-телефонії в корпоративних мережах є важливою та актуальною, оскільки від її вирішення залежить не лише захист персональних даних користувачів, але й цілісність інформаційних потоків в організації. Нестабільність у роботі систем IP-телефонії може призвести до непередбачуваних збоїв у роботі бізнесу, що є неприпустимим у сучасних умовах конкурентного середовища.

Отже, необхідно розробити ефективні методи та інструменти забезпечення безпеки, які дозволяють знизити вразливості системи та забезпечити надійність та конфіденційність комунікацій.

Метою стало дослідження сучасних підходів до забезпечення безпеки IP-телефонії, аналіз наявних технічних рішень і формування рекомендацій щодо побудови ефективної підсистеми захисту для корпоративного середовища.

Об'єктом дослідження є система забезпечення безпеки використання IPтелефонії в корпоративних мережах, а предметом дослідження – методи, засоби та механізми захисту IP-телефонії в умовах сучасних загрозінформаційній безпеці.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В IP-ТЕЛЕФОНІЇ

1.1. Поняття IP-телефонії та особливості її застосування у корпоративних мережах

1.1.1 Визначення IP-телефонії (VoIP)

IP-телефонія (Voice over Internet Protocol, VoIP) - це сучасний метод, що дозволяє передавати голосові дані за допомогою IP-мереж, на зразок локальних мереж (LAN) чи Інтернету. Вона перетворює голосові сигнали на цифрові потоки даних, даючи змогу об'єднати телефонні послуги та комп'ютерні мережі на одній платформі. IP-телефонія охоплює мережеве обладнання, програмне забезпечення для обробки сигналів, мережеві протоколи і служби для управління зв'язком в реальному часі.

Експерти з Cisco Systems та фахівці з Avaya вважають IP-телефонію логічним кроком еволюції телекомунікацій, де акцент переміщується з класичних аналогових систем зв'язку на інтегровані цифрові рішення. Прикладами таких рішень є корпоративні АТС на базі IP (IP-PBX), системи для відеоконференцій, програмні SIP-клієнти, а також інтегровані системи уніфікованих комунікацій (Unified Communications)

Основні риси IP-телефонії:

Цифрове кодування голосу – перетворення аналогового голосу в цифровий формат.

Об'єднання з комп'ютерними мережами – використання вже наявної мережевої інфраструктури.

Гнучкість та масштабованість – швидке налаштування і розширення корпоративних телефонних систем.

Економія ресурсів – зменшення витрат на телефонний зв'язок завдяки передачі голосу через IP-мережі.

Підтримка додаткових послуг – голосові повідомлення, переадресація викликів, конференц-зв'язок, запис розмов та інше.

1.1.2 Інфраструктура IP-телефонії у корпоративних мережах

Типова система IP-телефонії у корпоративному середовищі включає такі ключові компоненти:

Кінцеві точки: IP-телефони, програмні SIP-клієнти (наприклад, Zoiper, 3CX).

Сервери: IP-PBX (наприклад, Asterisk, FreePBX, Cisco Unified Communications Manager).

Мережеві комутатори (Switches): з функцією QoS (Quality of Service) для гарантування якості звуку.

Мережеві шлюзи (Gateways): пристрої для зв'язку між IP-телефонією та звичайними телефонними мережами (PSTN).

Протоколи: SIP, RTP, RTCP, SRTP, TLS та інші.

Корпоративні IP-телефонні рішення часто інтегруються з CRM-системами, системами електронного документообігу та іншим бізнес-софтом, що дає змогу автоматизувати комунікації та підвищити ефективність роботи співробітників, продемонстровано в додатку Г.

1.1.3 Проблематика безпеки IP-телефонії

Збільшення впровадження IP-телефонії в корпоративних мережах зумовлює виникнення нових загроз у галузі інформаційної безпеки. Голосовий потік, який передається через IP-мережі, може бути чутливим до різних загроз, зокрема, прослуховування розмов, підміна викликів, DDoS-атаки та інші.

Ключові загрози для корпоративної IP-телефонії включають:

Перехоплення голосового трафіку (Eavesdropping) - несанкціоноване отримання доступу до розмов.

Підробка ідентифікації абонента (Caller ID spoofing) - маніпулювання інформацією про абонента, що телефонує.

Відмова в обслуговуванні (DoS/DDoS-атаки) - перевантаження серверу чи мережі, яке перешкоджає нормальній роботі VoIP-системи.

Несанкціонований доступ (Unauthorized access) - зламування облікових записів користувачів або адміністраторів IP-телефонії.

Фішинг через VoIP (Vishing) - соціальна інженерія з використанням IP-телефонії для отримання конфіденційних даних.

Зважаючи на зазначені ризики, стає вкрай важливим створення дієвої підсистеми забезпечення безпеки IP-телефонії.

1.1.4 Вимоги до системи безпеки IP-телефонії

Сучасні стратегії захисту IP-телефонії в корпоративному середовищі зобов'язані відповідати ключовим критеріям:

Конфіденційність: голосовий трафік необхідно оберігати від неправомірного проникнення за допомогою криптографічного захисту.

Цілісність: голосові дані мають бути передані без змін чи втрат, гарантуючи їхню достовірність.

Доступність: забезпечення безперервного функціонування та надійності сервісів IP-телефонії.

Автентифікація та авторизація: ідентифікація абонентів та регулювання доступу до ресурсів IP-телефонії.

Облік і аудит: фіксація дій користувачів та ведення журналів дзвінків для аналізу та реагування на потенційні загрози безпеки.

1.1.5 Приклади реалізації безпечної IP-телефонії

Вдалі приклади застосування захищеної IP-телефонії можна зустріти у багатьох глобальних корпораціях:

Cisco Systems - використовує Cisco Unified Communications Manager разом із Secure RTP (SRTP) та TLS, що гарантує шифрування аудіо потоків та сигнальних потоків.

Microsoft Teams - корпоративна платформа, що об'єднує IP-телефонію з шифруванням та багатошаровим захистом облікових записів.

Asterisk – широко використовувана IP-PBX система з відкритим вихідним кодом, що підтримує широкий спектр технологій безпеки, включно з шифруванням та аутентифікацією SIP-підключень.

В Україні подібні рішення активно впроваджуються в банківському секторі, великих IT-компаніях та державних організаціях, де питання безпеки комунікацій є першочерговим.

1.2 Методи забезпечення безпеки інформаційних систем

Методи забезпечення безпеки інформаційних систем є набором стратегій та підходів, що використовуються для реалізації захисних функцій та ефективної протидії актуальним кіберзагрозам. Ці методи, поєднуючи технічні, програмні та організаційні аспекти, дозволяють створити багаторівневу, ешелоновану систему захисту. В контексті IP-телефонії в корпоративній мережі виділяють наступні ключові методи:

1.2.1 Криптографічні методи захисту інформації та забезпечення конфіденційності

Криптографія є фундаментальним методом для гарантування конфіденційності та цілісності даних, що особливо важливо для голосових комунікацій, які можуть містити конфіденційну інформацію.

Шифрування сигнального трафіку за допомогою TLS (Transport Layer Security): протокол SIP (Session Initiation Protocol), який є основою для встановлення та управління сеансами IP-телефонії, початково не передбачає шифрування. Це

робить його вразливим для перехоплення метаданих дзвінків, даних авторизації та інших конфіденційних відомостей. Використання TLS дозволяє створити захищений канал зв'язку для SIP-трафіку, забезпечуючи конфіденційність, цілісність та автентифікацію між кінцевими точками. TLS використовує асиметричне шифрування для встановлення захищеної сесії та симетричне шифрування для подальшої передачі даних, захищаючи від атак типу "людина посередині" на етапі встановлення з'єднання.

Шифрування медіаданих за допомогою SRTP (Secure Real-time Transport Protocol): голосовий та відео трафік в IP-телефонії передається за протоколом RTP (Real-time Transport Protocol), який також не має вбудованих механізмів шифрування. SRTP розширює RTP, додаючи функції шифрування, автентифікації та захисту від повторів для голосових пакетів. Це гарантує конфіденційність змісту розмов та захист від їх спотворення. Кожен дзвінок отримує унікальний криптографічний ключ, що ускладнює прослуховування навіть у разі компрометації одного ключа.

Використання VPN-тунелів (Virtual Private Network) VPN створює зашифрований, логічно ізольований "тунель" через публічні, незахищені мережі. Весь трафік IP-телефонії, що проходить через VPN-тунель, шифрується та інкапсулюється, забезпечуючи конфіденційність, цілісність та автентифікацію. Це особливо ефективно для захисту комунікацій віддалених працівників, філій або при з'єднанні з SIP-операторами, де пряме підключення може бути вразливим. VPN також допомагає обійти блокування портів або протоколів інтернет-провайдерами.

1.2.2 Методи контролю доступу та автентифікації/авторизації

Ці методи є основою для забезпечення того, що доступ до ресурсів системи IP-телефонії отримують лише авторизовані користувачі та пристрої.

Надійна автентифікація: включає використання стійких до злому паролів, які є довгими, складними, містять комбінації літер, цифр та спеціальних символів, та регулярно оновлюються.

Застосування багатофакторної автентифікації (MFA), яка вимагає від користувача надання двох або більше різних типів доказів ідентичності (наприклад, пароль + код з SMS), значно підвищує безпеку. Також важливим є блокування IP-адрес після кількох невдалих спроб входу.

Авторизація та рольові моделі доступу (RBAC - Role-Based Access Control): після автентифікації користувачу надаються певні права та привілеї на основі його ролі у компанії. RBAC гарантує, що співробітники мають доступ лише до тих функцій та ресурсів IP-телефонії, які необхідні для виконання їхніх обов'язків. Наприклад, деяким користувачам може бути дозволено лише здійснювати внутрішні дзвінки, іншим - міжнародні, а адміністраторам - повне управління системою. Це обмежує потенційний збиток у разі компрометації облікового запису.

Обмеження доступу за IP-адресами: налаштування системи IP-телефонії для дозволу підключення лише з заздалегідь визначених, довірених IP-адрес. Це ефективний спосіб запобігти несанкціонованим спробам доступу ззовні, обмежуючи коло потенційних атакуючих.

1.2.3 Методи мережевого захисту

Мережева безпека формує базовий рівень захисту для всієї інформаційної системи, включаючи IP-телефонію, оскільки VoIP функціонує поверх IP-мереж.

Брандмауери (Firewalls): є першим ешелоном оборони, контролюючи вхідний та вихідний мережевий трафік на основі встановлених правил безпеки. Вони фільтрують пакети даних, блокуючи небажані або підозрілі з'єднання, що можуть бути частиною атаки. Брандмауери можуть працювати на різних рівнях моделі OSI та бути інтегрованими як програмно так і апаратно.

Session Border Controllers (SBC): контролери сеансів межі є високоспеціалізованими мережевими пристроями, розробленими для захисту та управління VoIP-трафіком на межі корпоративної мережі та зовнішніх мереж. SBC виконують широкий спектр функцій безпеки, виступаючи як багатофункціональний шлюз та захисний бар'єр:

– NAT Traversal: Дозволяють коректно функціонувати VoIP-трафіку через пристрої мережевої адресної трансляції NAT, що є типовою проблемою для SIP-протоколу.

– Захист від DoS/DDoS-атак: SBC активно моніторять та контролюють кількість одночасних з'єднань та швидкість SIP-повідомлень, що надходять до мережі. Це запобігає перевантаженню IP-АТС та інших внутрішніх ресурсів під час DoS/DDoS-атак, відхиляючи підозрілий трафік на межі мережі.

– Приховування топології мережі: SBC маскує внутрішню архітектуру корпоративної мережі, переховуючи внутрішні IP-адреси та структуру IP-телефонії. Це ускладнює зловмисникам дослідження мережі та планування цілеспрямованих атак.

– Шифрування та автентифікація на межі мережі: SBC можуть виконувати функції шифрування TLS/SRTP та автентифікації для зовнішніх з'єднань, забезпечуючи безпеку трафіку, що входить або виходить з корпоративної мережі.

– Фільтрація та нормалізація SIP-трафіку: SBC можуть виконувати глибоку перевірку SIP-пакетів, відкидаючи некоректні або зловмисні запити, які можуть бути частиною атак, таких як SPIT або Fuzzing.

–

1.2.4 Методи виявлення та запобігання вторгненням

Ці методи сфокусовані на проактивному моніторингу, виявленні та блокуванні шкідливої або аномальної активності в режимі реального часу.

Системи виявлення вторгнень (IDS - Intrusion Detection Systems) та системи запобігання вторгненням (IPS - Intrusion Prevention Systems): IDS пасивно моніторять мережевий трафік та системні журнали, порівнюючи їх з відомими сигнатурами атак або виявляючи аномальну поведінку, та генерують попередження для адміністраторів. IPS, на відміну від IDS, мають можливість активно блокувати підозрілу активність, щойно її виявлено, запобігаючи проникненню або поширенню

атаки. Вони можуть працювати на мережевому рівні (NIDS/NIPS) або на хості (HIDS/HIPS).

Аналіз логів та автоматичне блокування IP-адрес: Постійний моніторинг та аналіз системних журналів (логів) IP-АТС (наприклад, Asterisk, FreePBX), шлюзів та інших компонентів IP-телефонії є життєво важливим. Журнали містять інформацію про всі події, включаючи спроби входу, дзвінки, помилки та підозрілу активність. Використання інструментів, таких як Fail2Ban, дозволяє автоматично аналізувати ці логи за допомогою регулярних виразів. У разі виявлення багаторазових невдалих спроб входу, сканування портів або ознак DoS-атак (наприклад, великої кількості SIP UDP пакетів з одного джерела), Fail2Ban може автоматично блокувати IP-адресу зловмисника за допомогою правил фаєрволу (наприклад, iptables). Це є дуже ефективним методом захисту від атак підбору паролів та відмови в обслуговуванні.

1.2.5 Організаційні та процедурні методи захисту

Людський фактор та організаційні недоліки часто є найслабшою ланкою в системі безпеки. Тому ці методи є не менш важливими, ніж технічні:

Розробка та впровадження політик безпеки: створення чітких, документованих політик та процедур, які регламентують усі аспекти використання IP-телефонії: правила створення та зміни паролів, процедури доступу до конфіденційної інформації, порядок реагування на інциденти безпеки, правила використання кінцевих пристроїв (IP-телефонів, софтфонів). Ці політики мають бути обов'язковими для всіх співробітників.

Навчання та підвищення обізнаності співробітників: регулярне навчання персоналу щодо актуальних кіберзагроз (фішинг, соціальна інженерія, SPIT, спуфінг), важливості використання надійних паролів, обережності при роботі з підозрілими дзвінками або повідомленнями. Підвищення обізнаності допомагає запобігти багатьом інцидентам, спричиненим людськими помилками або незнанням.

Регулярне оновлення програмного забезпечення та патчінг: вчасне встановлення оновлень та патчів безпеки для IP-АТС, кінцевих пристроїв (IP-

телефонів, шлюзів), операційних систем на серверах та мережевому обладнанні є життєво важливим. Розробники постійно виявляють та виправляють вразливості, і їх своєчасне усунення значно підвищує рівень захисту від відомих атак.

Резервне копіювання даних: регулярне створення резервних копій конфігурацій IP-АТС, баз даних користувачів, журналів подій та інших критично важливих даних. Це дозволяє швидко відновити систему після збою, кібератаки або іншої катастрофи, мінімізуючи час простою та фінансові втрати, що є ключовим для забезпечення доступності сервісу.

Фізична безпека: забезпечення контрольованого доступу до серверних приміщень, комунікаційних шаф та іншого обладнання, що є частиною інфраструктури IP-телефонії. Це запобігає несанкціонованому фізичному доступу, крадіжкам, саботажу або маніпуляціям з обладнанням.

Аудит та моніторинг: Регулярний аудит систем безпеки, моніторинг мережевого трафіку та активності користувачів дозволяють вчасно виявляти відхилення від нормальної роботи та потенційні загрози.

Застосування цих методів у комплексі, у відповідності до архітектурних принципів, дозволяє створити багатошарову, ешелоновану систему захисту IP-телефонії. Це забезпечує ефективне протистояння широкому спектру кіберзагроз, мінімізуючи ризики для конфіденційності, цілісності та доступності комунікацій в корпоративній мережі.

1.2.6 Методології управління ризиками інформаційної безпеки

Для системного підходу до забезпечення безпеки ІС, включно з IP-телефонією, застосовуються спеціалізовані методології управління ризиками. Ці методології дозволяють організаціям ідентифікувати, оцінювати, обробляти та моніторити ризики інформаційної безпеки, забезпечуючи раціональне розподілення ресурсів для захисту.

Серед найбільш відомих методологій, що згадуються в контексті управління ризиками інформаційної безпеки, можна виділити:

FRAP (Facilitated Risk Analysis Process): цей підхід є спрощеним методом якісного аналізу ризиків, який фокусується на найбільш критично важливих активах інформаційної системи. Він передбачає використання експертної оцінки для швидкого визначення основних загроз та вразливостей, що дозволяє оперативно реагувати на найбільш значущі ризики. FRAP є корисним для початкової оцінки або для швидкого аудиту безпеки IP-телефонії у корпоративній мережі, щоб виявити найбільш очевидні "дірки".

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): методологія OCTAVE зосереджена на самооцінці ризиків інформаційної безпеки, яку проводять безпосередньо бізнес-підрозділи компанії. Вона забезпечує комплексний погляд на інформаційні системи та бізнес-процеси, дозволяючи ідентифікувати активи, загрози, вразливості та розробляти стратегії зниження ризиків. OCTAVE є особливо цінною для великих організацій, оскільки вона дозволяє залучити до процесу оцінки ризиків тих, хто безпосередньо працює з інформаційними активами, включаючи користувачів IP-телефонії та її адміністраторів.

FMEA (Failure Modes and Effect Analysis): аналіз видів та наслідків відмов є методологією, спрямованою на оцінку слабких сторін системи з метою ідентифікації ненадійних елементів або потенційних точок відмови. У контексті IP-телефонії FMEA може бути використана для аналізу компонентів системи (наприклад, серверів IP-АТС, шлюзів, мережевого обладнання) та виявлення потенційних відмов, які можуть призвести до порушення доступності зв'язку або інших проблем безпеки. Це дозволяє проактивно вживати заходів для підвищення надійності та стійкості.

CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method): ця методологія використовує автоматизовані інструменти для управління ризиками інформаційної безпеки. CRAMM є більш структурованим та формалізованим підходом, що дозволяє проводити детальну оцінку ризиків та розробляти відповідні заходи захисту. Вона може бути корисною для комплексного аудиту безпеки IP-телефонії та розробки довгострокових стратегій захисту.

NIST (National Institute of Standards and Technology): національний інститут стандартів і технологій США розробив низку публікацій (наприклад, NIST Special Publication 800-30), які містять детальні рекомендації з управління ризиками інформаційної безпеки. Методологія NIST передбачає оцінку потенційного збитку від реалізації загроз та ймовірності їх виникнення, що дозволяє пріоритезувати ризики та вибирати найбільш ефективні заходи контролю.

Застосування цих методологій дозволяє не лише реагувати на існуючі загрози, а й проактивно виявляти потенційні ризики, розробляти стратегії їх мінімізації та впроваджувати обґрунтовані заходи безпеки, що є ключовим для побудови надійної підсистеми забезпечення безпеки IP-телефонії.

1.3 Постановка задачі

Основною метою даної дипломної роботи є розробка та наукове обґрунтування принципів побудови ефективної та надійної підсистеми забезпечення безпеки IP-телефонії в корпоративній мережі. Ця підсистема має бути спроектована таким чином, щоб адекватно протидіяти існуючим та потенційним загрозам, забезпечуючи на всіх рівнях захисту конфіденційність, цілісність та доступність голосових та сигнальних даних.

Для досягнення поставленої мети необхідно вирішити наступні основні завдання:

1. Провести поглиблений аналіз архітектури IP-телефонії та її взаємодії з корпоративною мережею:

Дослідити ключові компоненти системи IP-телефонії (IP-АТС, шлюзи, IP-телефони, софтфони, протоколи SIP, RTP).

Визначити основні точки взаємодії IP-телефонії з іншими елементами корпоративної мережі (маршрутизатори, комутатори, сервери, робочі станції) та зовнішніми мережами.

Проаналізувати типові сценарії розгортання IP-телефонії в корпоративному середовищі.

2. Виконати всебічний аналіз актуальних загроз та вразливостей безпеки IP-телефонії в корпоративних мережах:

Систематизувати та детально описати різні категорії кіберзагроз, спрямованих на IP-телефонію, включаючи атаки на конфіденційність (прослуховування, перехоплення), цілісність (спуфінг, модифікація даних) та доступність (DoS/DDoS, SPIT, фрікінг).

3. Дослідити та систематизувати сучасні методи та засоби забезпечення безпеки інформаційних систем, придатні для IP-телефонії:

Проаналізувати ефективність криптографічних протоколів (TLS для SIP, SRTP для RTP) у забезпеченні конфіденційності та цілісності голосового трафіку.

Розглянути роль мережевих засобів захисту, таких як міжмережеві екрани (брандмауери), віртуальні приватні мережі (VPN), а також спеціалізовані Session Border Controllers (SBC) у захисті VoIP-мереж від зовнішніх атак та управлінні трафіком.

Дослідити принципи функціонування систем виявлення та запобігання вторгненням (IDS/IPS) та їх застосування для моніторингу та блокування аномальної активності в IP-телефонії, включаючи програмні інструменти типу Fail2Ban.

Описати організаційно-правові та адміністративні заходи безпеки, такі як розробка політик безпеки, управління доступом, регулярне оновлення програмного забезпечення, резервне копіювання, а також навчання персоналу та підвищення їхньої обізнаності щодо кіберзагроз.

Проаналізувати застосування методологій управління ризиками інформаційної безпеки (наприклад, OCTAVE, NIST) для систем IP-телефонії.

4. Обґрунтувати архітектурні принципи побудови та функціонування підсистеми забезпечення безпеки IP-телефонії в корпоративній мережі:

Розробити концептуальну модель підсистеми безпеки, яка базуватиметься на принципах багатошаровості, ешелонованої оборони (багатозональність, багаторубіжність) та мінімальної достатності.

Визначити оптимальне розміщення та взаємодію ключових компонентів захисту (SBC, брандмауерів, IDS/IPS, механізмів шифрування) в типовій корпоративній мережі для забезпечення ефективного захисту на всіх рівнях.

Запропонувати принципи інтеграції підсистеми безпеки IP-телефонії з існуючою системою управління інформаційною безпекою підприємства.

5. Розробити практичні рекомендації щодо впровадження та підтримки підсистеми забезпечення безпеки IP-телефонії:

Надати конкретні технічні рекомендації щодо конфігурації IP-АТС, мережевого обладнання та кінцевих пристроїв для підвищення їхньої стійкості до атак.

Сформулювати настанови щодо моніторингу стану безпеки, швидкого реагування на інциденти та проведення регулярного аудиту системи IP-телефонії.

Запропонувати заходи з підвищення обізнаності користувачів та адміністраторів щодо правил безпечної роботи з IP-телефонією.

Об'єктом дослідження є процеси забезпечення безпеки інформації в системах IP-телефонії. Предметом дослідження є методи, засоби та принципи побудови комплексної підсистеми забезпечення безпеки використання IP-телефонії в корпоративній мережі.

Результати даної роботи дозволять розробити теоретичні та практичні засади для створення надійної та ефективної системи захисту IP-телефонії, що сприятиме стабільному функціонуванню бізнес-комунікацій, мінімізації кіберризиків та захисту конфіденційних даних в сучасному корпоративному середовищі.

1.4 Висновки до першого розділу

У першому розділі кваліфікаційної роботи було всебічно досліджено теоретичні основи та засадничі аспекти забезпечення безпеки систем IP-телефонії в контексті їх застосування у корпоративних мережах.

На початку розділу було надано чітке визначення IP-телефонії (VoIP), розкрито її ключові особливості та переваги, такі як цифрова кодифікація голосу,

об'єднання з комп'ютерними мережами, гнучкість, масштабованість, мультимедійність та економічна ефективність. Проаналізовано принципи роботи основних протоколів (SIP, RTP), що є фундаментальними для розуміння функціонування та потенційних вразливостей VoIP-систем.

Критично важливим аспектом дослідження стало виявлення та класифікація загроз і вразливостей, характерних для IP-телефонії. Визначено, що інтеграція голосового трафіку в IP-мережі створює нові ризики, пов'язані з прослуховуванням, перехопленням, підробкою ідентифікаторів, DoS/DDoS-атаками, несанкціонованим доступом та використанням шкідливого програмного забезпечення. Особливу увагу приділено впливу цих загроз на конфіденційність, цілісність та доступність інформації.

Проаналізовано існуючі методи та засоби захисту IP-телефонії, включаючи криптографічні методи (шифрування SIP та RTP за допомогою TLS та SRTP), механізми автентифікації та авторизації, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), а також віртуальні приватні мережі (VPN). Висвітлено роль управління ідентифікацією та доступом, сегментації мережі, моніторингу та аудиту в забезпеченні комплексної безпеки.

Наприкінці розділу було сформульовано основні принципи побудови комплексної підсистеми забезпечення безпеки IP-телефонії, такі як безперервність захисту, ешелонована оборона та мінімальна достатність. Визначено об'єкт (процеси забезпечення безпеки інформації в системах IP-телефонії) та предмет дослідження (методи, засоби та принципи побудови комплексної підсистеми) кваліфікаційної роботи.

Таким чином, перший розділ закладає необхідний теоретичний фундамент для подальшого проектування та практичної реалізації підсистеми забезпечення безпеки IP-телефонії, надаючи всебічне розуміння проблеми та шляхів її вирішення.

2 ПІДСИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ ДЛЯ БЕЗПЕЧНОГО ВИКОРИСТАННЯ В МЕРЕЖАХ КОМПАНІЙ

Сучасні технології зв'язку розвиваються дуже швидко, і це відкриває багато можливостей для компаній. Але разом з тим з'являються й нові проблеми з безпекою даних. IP-телефонія, яка передає голос через інтернет, стала дуже популярною завдяки своїй гнучкості, масштабованості та економії. Проте, ці ж переваги роблять її вразливою до різних хакерських атак. Тому зараз дуже важливо розробити надійну систему, яка б захищала IP-телефонію. Для цього треба розібратися в сучасних рішеннях, оцінити можливі загрози, вибрати найкращі методи захисту і спроектувати таку архітектуру, яка буде підходити для реальних корпоративних умов.

Щоб побудувати систему захисту IP-телефонії, потрібен комплексний підхід, який забезпечить конфіденційність інформації, що передається через мережу. Оскільки голосовий зв'язок дуже активно використовується в організаціях, важливо мати ефективні методи захисту від усіх можливих загроз. Система захисту IP-телефонії повинна включати механізми, які б гарантували конфіденційність, цілісність і доступність переданих даних. Це означає, що треба використовувати криптографію для шифрування голосових повідомлень і методи аутентифікації, щоб перевіряти, хто саме розмовляє. Також одне з ключових завдань – це захист від атак, таких як "відмова в обслуговуванні" (DoS) або несанкціоноване перехоплення даних.

2.1 Аналіз архітектури та вразливостей IP-телефонії в контексті корпоративного середовища

Впровадження IP-телефонії (Voice over IP, VoIP) у корпоративній мережі забезпечує значні переваги з точки зору гнучкості, масштабованості та економії коштів порівняно з традиційними телефонними системами. Однак, перехід від ізольованих аналогових або цифрових телефонних мереж до інтегрованої IP-

інфраструктури виводить голосовий трафік у відкрите мережеве середовище, що створює низку нових загроз та вразливостей. Розуміння архітектурних особливостей VoIP-систем та їхніх потенційних слабких місць є першочерговим кроком у проектуванні ефективної підсистеми безпеки.

Типова архітектура корпоративної IP-телефонії включає такі ключові компоненти, кожен з яких може бути потенційною мішенню для атак:

Сервер IP-телефонії (IP-АТС, Softswitch, Call Manager): це центральний вузол системи, який відповідає за реєстрацію абонентів, маршрутизацію дзвінків, управління з'єднаннями та надання додаткових сервісів. У даній роботі як основну платформу розглядається Asterisk, яка є програмною IP-АТС з відкритим кодом. Asterisk обробляє як сигналізаційний трафік (SIP), так і медіа-трафік (RTP), зберігає облікові дані користувачів, конфігурації та історію дзвінків. Його компрометація може призвести до повного порушення роботи системи, несанкціонованого доступу до розмов та іншої конфіденційної інформації.

Кінцеві пристрої (IP-телефони, софтфони): це апаратні або програмні клієнти, через які користувачі здійснюють та приймають дзвінки. Вони взаємодіють з SIP-сервером для реєстрації та встановлення з'єднань, а також обробляють голосовий трафік. Вразливості цих пристроїв (наприклад, слабкі паролі, необновлені прошивки, шкідливе програмне забезпечення на софтфонах) можуть слугувати точкою входу для зловмисників.

Голосові шлюзи (VoIP Gateways): пристрої, що забезпечують взаємодію IP-телефонії з традиційними телефонними мережами загального користування (ТМЗК). Вони перетворюють IP-пакети на аналогові / цифрові сигнали і навпаки. Безпека шлюзів важлива для запобігання несанкціонованому доступу до ТМЗК або перехоплення трафіку між мережами.

Мережева інфраструктура: включає комутатори, маршрутизатори та міжмережеві екрани, які забезпечують передачу IP-пакетів по мережі. Неправильне налаштування мережевого обладнання, відсутність сегментації трафіку (наприклад, окремих VLAN для VoIP) створює умови для перехоплення або модифікації голосового трафіку.

Ключові вразливості IP-телефонії, які підлягають усуненню:

Вразливості IP-телефонії виникають через природу використовуваних протоколів (SIP для сигналізації, RTP для медіа-трафіку) та їхню інтеграцію в загальну IP-мережу.

Вразливості протоколів сигналізації (SIP):

Несанкціонована реєстрація та підбір облікових даних (Brute-Force): Зловмисник може намагатися зареєструватися на SIP-сервері, використовуючи скомпрометовані або підібрані облікові дані. Успішна реєстрація дозволяє здійснювати дзвінки за рахунок компанії, прослуховувати розмови або навіть ініціювати атаки на інших користувачів. Ці атаки часто автоматизовані і полягають у переборі великої кількості комбінацій логінів/паролів.

Реєстраційне сканування: зловмисник надсилає велику кількість SIP-запитів REGISTER на різні потенційні абонентські номери для виявлення діючих облікових записів. Це може використовуватися для подальших атак або як елемент розвідки.

Підробка ідентифікатора абонента (Caller ID Spoofing): зловмисник може змінити відображуваний номер телефону, щоб видати себе за іншого користувача або відділ. Це може використовуватися для соціальної інженерії, фішингу або обходу систем безпеки.

Відмова в обслуговуванні (DoS/DDoS атаки): перевантаження SIP-сервера надмірною кількістю запитів (наприклад, INVITE, REGISTER) може вивести його з ладу або значно уповільнити роботу, роблячи телефонний зв'язок недоступним. Це може бути пряма атака на сам сервер або ж атака на службу NAT, яка використовується для маршрутизації трафіку, що призводить до відмови в обслуговуванні легітимних абонентів.

Вразливості голосового трафіку (RTP):

Перехоплення трафіку (Eavesdropping): за замовчуванням RTP-трафік не шифрується і передається у відкритому вигляді. Це дозволяє будь-якому зловмиснику в мережі, який має доступ до трафіку, прослуховувати розмови за допомогою звичайних мережевих аналізаторів.

Модифікація/впровадження трафіку (Tampering/Injection): якщо цілісність RTP-пакетів не захищена, зловмисник може впроваджувати шкідливі аудіофрагменти або спотворювати голосові дані в реальному часі, що може призвести до дезінформації або збоїв.

Вразливості мережевої інфраструктури та операційної системи:

Неправильна конфігурація міжмережевих екранів (Firewall): дозволяє несанкціонований доступ до SIP-сервера та інших внутрішніх ресурсів ззовні або з неавторизованих сегментів внутрішньої мережі.

Використання стандартних портів та облікових даних: залишення стандартних портів (наприклад, SSH 22, SIP 5060) та використання слабких або типових паролів спрощує атаки за сценаріями.

Відсутність сегментації мережі: якщо VoIP-трафік не відокремлений від інших даних, це збільшує ризик перехоплення та впливу на інші сервіси.

Вразливості в протоколах управління (наприклад, SSH): компрометація доступу до сервера через SSH може дати зловмиснику повний контроль над системою. Атаки brute-force на SSH є поширеними.

Враховуючи ці вразливості, проектування підсистеми безпеки вимагає комплексного підходу, що включає як захист протоколів SIP та RTP, так і убезпечення серверного середовища та мережевої інфраструктури, що обслуговує IP-телефонію.

2.2 Методологія проектування та розробки підсистеми забезпечення безпеки IP-телефонії

Методологія проектування підсистеми забезпечення безпеки IP-телефонії базується на ітеративному підході, який включає фази аналізу, проектування, реалізації та тестування. Кожен етап детально розглядає аспекти безпеки, що дозволяє створити надійне та ефективне рішення, яке відповідає специфічним загрозам корпоративного середовища.

2.2.1 Етап аналізу та формування вимог

На цьому етапі проводиться всебічне дослідження поточної IP-телефонної інфраструктури (якщо вона вже існує або планується), визначення потреб бізнесу та безпеки, а також ідентифікація потенційних загроз та вразливостей.

Аналіз поточної інфраструктури IP-телефонії:

Інвентаризація компонентів: визначення всіх апаратних (сервери, шлюзи, IP-телефони) та програмних (операційні системи, версії Asterisk, додаткові модулі) елементів системи IP-телефонії.

Аналіз мережевої топології: створення схеми мережі з позначенням розташування серверів, кінцевих пристроїв, маршрутизаторів, міжмережевих екранів, а також маршрутів SIP та RTP трафіку. Визначення VLAN-ів (якщо вони використовуються) або сегментів мережі.

Аналіз поточних конфігурацій: перевірка налаштувань безпеки на всіх пристроях: політики паролів, відкриті порти, правила міжмережевих екранів, наявність оновлень програмного забезпечення та прошивок.

Оцінка поточних ризиків: визначення існуючих прогалин у безпеці, які можуть бути використані зловмисниками (наприклад, відсутність шифрування, слабкі паролі, відкриті адміністративні порти).

Ідентифікація та класифікація загроз:

На основі аналізу архітектури та загальновідомих вразливостей IP-телефонії, формується конкретний перелік загроз, релевантних для даної корпоративної мережі. Кожна загроза класифікується за джерелом (зовнішня/внутрішня), типом впливу (порушення конфіденційності, цілісності, доступності) та рівнем ризику.

Особливий акцент робиться на загрозах, які планується усувати:

- несанкціонована реєстрація та brute-force атаки на SIP-акаунти;
- реєстраційне сканування мережі;
- атаки на службу NAT;
- перехоплення SIP та RTP трафіку;
- DoS-атаки на SIP-сервер;

– вразливості віддаленого доступу (SSH).

Формування вимог до підсистеми безпеки:

Функціональні вимоги:

– підсистема повинна забезпечувати шифрування сигналізаційного (SIP) трафіку за допомогою TLS;

– підсистема повинна забезпечувати шифрування медіа-трафіку (RTP) за допомогою SRTP;

– підсистема повинна забезпечувати автентифікацію клієнтів (IP-телефонів/софтфонів) до Asterisk-сервера;

– підсистема повинна захищати від несанкціонованих підключень до SIP-сервера;

– підсистема повинна виявляти та блокувати brute-force атаки на SIP-акаунти;

– підсистема повинна забезпечувати захист від DoS-атак;

– підсистема повинна забезпечувати захист від атак на службу NAT;

– підсистема повинна забезпечувати безпечний віддалений доступ до сервера (SSH);

– підсистема повинна вести журнал подій безпеки для подальшого аналізу.

Нефункціональні вимоги:

– продуктивність (впроваджені заходи безпеки не п овинні суттєво впливати на якість голосового зв'язку (затримка, джиттер, втрата пакетів);

– надійність (підсистема безпеки повинна бути стабільною та не створювати єдиної точки відмови);

– масштабованість (рішення повинні бути масштабованими для підтримки зростаючої кількості абонентів та трафіку);

– сумісність (засоби безпеки повинні бути сумісними з обраною платформою Asterisk та наявними IP-телефонами);

– керованість (наявність зрозумілих механізмів конфігурації та моніторингу);

– економічна ефективність (використання Open Source рішень для мінімізації витрат на ліцензування).

2.2.2 Етап проектування підсистеми безпеки

На етапі проектування розробляється детальна архітектура підсистеми безпеки, обираються конкретні програмні та апаратні засоби, а також визначаються методи їх інтеграції.

Розробка архітектури підсистеми безпеки:

Централізований підхід на базі Asterisk, де підсистема безпеки буде інтегрована безпосередньо з Asterisk-сервером та операційною системою хоста (Linux), використовуючи вбудовані можливості та додаткові програмні засоби.

Багаторівневий захист – архітектура передбачає захист на різних рівнях:

– рівень додатків/протоколів (SIP/RTP) забезпечується безпосередньо Asterisk за допомогою TLS та SRTP;

– рівень операційної системи, який передбачає захист хоста Asterisk через конфігурацію SSH та використання Fail2Ban;

– мережевий рівень, на якому здійснюється захист за допомогою вбудованого міжмережевого екрана (iptables);

– розмежування мережевого трафіку рекомендовано, хоча це не є основною частиною реалізації в 3 розділі, в ідеалі, VoIP-трафік (SIP/RTP) слід відокремлювати від інших типів трафіку за допомогою VLAN-ів або окремих мережевих інтерфейсів, що знижує ризик несанкціонованого перехоплення та полегшує застосування політик міжмережевого екрана.

2.2.2.1 Платформа IP-телефонії: Asterisk

Обґрунтування вибору: Asterisk є гнучким, масштабованим програмним комутатором з відкритим вихідним кодом, що дозволяє реалізувати повноцінну IP-АТС. Він підтримує ключові протоколи (SIP, IAX) та має широкі можливості для

налаштування безпеки. Відкритий код дозволяє більш глибокий аудит та кастомізацію під специфічні вимоги корпоративної мережі, а також відсутність ліцензійних витрат робить його економічно вигідним рішенням.

Ключові можливості безпеки в Asterisk полягають в підтримці SIP over TLS (SIPS), можливості шифрування сигналізаційного трафіку; підтримці SRTP, можливості шифрування голосового медіа-трафіку; механізмах автентифікації SIP Digest; гнучкості налаштування доступу, можливості конфігурування правил доступу на рівні SIP-peers/users. Asterisk генерує докладні логи, які можуть бути використані для моніторингу та виявлення атак.

2.2.2.2 Засоби захисту операційної системи та мережевого рівня

Iptables є вбудованим міжмережевим екраном ядра Linux, що надає високий рівень контролю над мережевим трафіком. Це дозволяє ефективно фільтрувати пакети, обмежувати доступ до портів та сервісів, захищати від мережевих атак. Його інтеграція з операційною системою сервера Asterisk мінімізує додаткові апаратні витрати та спрощує конфігурацію. Зазначені характеристки пояснюють вибір Iptables.

Функціонал для безпеки IP-телефонії передбачає фільтрацію трафіку, надає дозвіл лише необхідних портів (SIP/TLS, RTP) та блокування всіх інших; обмеження доступу через дозвіл підключень лише з довірених IP-адрес або діапазонів; захист від DoS-атак, що створює можливість налаштування правил для відстеження кількості пакетів та блокування джерел з аномальною активністю; блокування ICMP – захист від сканування та інших мережевих атак, що використовують ICMP-пакети; NAT-захист, що передбачає допомогу у вирішенні проблем NAT traversal з одночасним підвищенням безпеки.

Ми надаємо обґрунтування вибору системи виявлення та запобігання вторгненням Fail2Ban (служба, що сканує файли журналів (логи) на наявність підозрілих активностей, таких як багаторазові невдалі спроби авторизації, та автоматично блокує відповідні IP-адреси за допомогою правил iptables). Це

ефективний інструмент для протидії brute-force атакам на SSH, Asterisk (SIP) та іншим сервісам.

Функціонал для безпеки IP-телефонії передбачає захист SSH через блокування IP-адрес, що намагаються підібрати паролі до SSH-доступу; рахист Asterisk/SIP, а саме моніторинг логів Asterisk на предмет невдалих спроб SIP-реєстрації або INVITE-запитів та блокування атакуючих IP-адрес; автоматичне блокування, що автоматизує процес блокування зловмисників, знижуючи навантаження на адміністратора.

Вважає доцільним вибір SSH як основного засобу віддаленого управління сервером. Його неправильна конфігурація може створити значну вразливість. Заходи, такі як зміна стандартного порту, заборона входу від імені root та використання окремих користувачів з обмеженими привілеями, є стандартними та ефективними практиками безпеки.

Функціонал для безпеки є наступним:

– зміна порту: ускладнює автоматизоване сканування та атаки;

– заборона входу root: запобігає прямим атакам на найбільш привілейований обліковий запис;

– використання sudo: дозволяє контрольоване підвищення привілеїв для звичайних користувачів, зменшуючи ризик компрометації системи.

2.2.2.3 Апаратні засоби

Серверна платформа: для розміщення Asterisk та компонентів безпеки потрібен сервер. Це може бути фізичний сервер або віртуальна машина з достатніми обчислювальними ресурсами (процесор, оперативна пам'ять, дисковий простір) для обробки голосового трафіку, шифрування та функціонування систем безпеки. Вибір конкретної конфігурації залежить від очікуваного навантаження (кількість одночасних дзвінків, абонентів).

IP-телефони / Софтфони: кінцеві пристрої, що підтримують SIP over TLS (SIPS) та SRTP. Більшість сучасних IP-телефонів мають такі можливості, але це необхідно перевіряти при виборі.

Планування інтеграції компонентів передбачає встановлення Asterisk на операційну систему, налаштування iptables безпосередньо в операційній системі сервера. Fail2Ban також встановлюється на сервері та інтегрується з логами Asterisk та системними логами. Конфігурації Asterisk (SIP-peers, extensions) модифікуються для підтримки TLS/SRTP. Кінцеві пристрої (IP-телефони) налаштовуються на використання SIPS та SRTP для взаємодії з Asterisk.

2.2.3 Етап реалізації та конфігурування

На цьому етапі відбувається безпосереднє впровадження спроектованих рішень. Детальний опис кроків реалізації, що слідує за цим підрозділом, знаходиться у розділі 3 вашої дипломної роботи. Тут ми лише визначаємо основні етапи та групи робіт.

Налаштування Asterisk для захищених комунікацій здійснюєтьсяпокроково. По-перше, відбувається генерація та конфігурація сертифікатів SSL/TLS щляхом створення ключів та сертифікатів (самопідписаних або від корпоративного CA) для Asterisk. Далі відбувається налаштування Asterisk на прослуховування TLS-портів (зазвичай 5061) та використання цих сертифікатів.

Конфігурація SIP-peers для TLS та SRTP здійснюється наступним чином: у файлах sip.conf (або pjsip.conf для PJSIP) в Asterisk налаштування параметрів transport=tls, encryption=yes, dtls=yes (для DTLS-SRTP).

Налаштування автентифікації клієнтів – забезпечення надійних паролів для SIP-акаунтів.

Базова політика безпеки передбачає наступне: встановлення політики за замовчуванням DROP для вхідних та вихідних з'єднань, що забезпечує максимальну безпеку.

Дозвіл необхідних портів передбачає вхідні з'єднання лише на порти:

SIP (5060 UDP/TCP, 5061 TCP для TLS), RTP (динамічний діапазон портів, наприклад, 10000-20000 UDP), SSH (змінений порт).

Необхідні також й інші сервіси (наприклад, HTTP/HTTPS для веб-інтерфейсу управління, якщо використовується, але з обмеженням доступу).

Наступне правило вказує на обмеження доступу за IP-адресами (створення правил, що дозволяють підключення до SIP та SSH лише з визначених IP-адрес або мереж (наприклад, внутрішньої корпоративної мережі).

Захист від DoS впроваджується через правила iptables для відстеження кількості пакетів та блокування джерел з аномальною активністю (наприклад, limit та recent модулі). Заборона ICMP – блокування або обмеження ICMP-запитів для зменшення можливостей мережевого сканування.

Налаштування безпечного віддаленого доступу (SSH) відбувається шляхом зміни порту SSH, редагування файлу /etc/ssh/sshd_config для зміни стандартного порту 22 на нестандартний (наприклад, 2222). Заборона входу root відбуваєтьбся через посередництво встановлення PermitRootLogin no у sshd_config.

Створення нового користувача з sudo відбувається шляхом додавання окремого користувача для адміністрування та надання йому прав sudo для виконання команд з підвищеними привілеями.

Налаштування Fail2Ban передбачає наступне:

- встановлення Fail2Ban (інсталяція пакета);
- конфігурація файлів jail.local;
- увімкнення «джаілів» (jail) для SSH (sshd) та Asterisk (asterisk).

Здійснюється визначення регулярних виразів (regex) для моніторингу логів Asterisk на предмет SIP-атак (brute-force, реєстраційне сканування). Впроваджується налаштування сповіщень (конфігурація відправлення електронних листів адміністратору при блокуванні IP-адрес).

Налаштування IP-телефонів / Софтфонів передбачає те, що кожен кінцевий пристрій повинен бути налаштований на використання TLS для SIP (порт 5061) та SRTP для голосового трафіку. Якщо використовуються сертифікати, підписані

корпоративним CA, кореневий сертифікат повинен бути завантажений на телефон для довіри до сервера.

2.2.4 Етап тестування та впровадження

Тестування є критично важливим етапом, що підтверджує ефективність впроваджених заходів безпеки. Функціональне тестування безпеки передбачає перевірку можливостей успішної реєстрації абонентів лише через TLS, перевірку шифрування голосового трафіку (наприклад, за допомогою Wireshark – спроби розшифрувати SRTP-трафік без ключів мають бути невдалими), перевірку коректної роботи автентифікації (неможливість зареєструватися зі слабкими/неправильними обліковими даними), тестування на проникнення (Penetration Testing), сканування портів, спроби перехоплення та модифікації трафіку, тестування продуктивності, оцінку затримок, джиттера та втрат пакетів при увімкнених механізмах шифрування. Ці показники не повинні виходити за межі допустимих значень для якісного голосового зв'язку.

Необхідне проведення навантажувальних тестів (наприклад, SIPp) для оцінки продуктивності Asterisk з увімкненою безпекою, моніторинг та аудит після впровадження, регулярний перегляд правил iptables та конфігурацій Asterisk для забезпечення актуальності та відповідності політиці безпеки, планування регулярних оновлень програмного забезпечення (Asterisk, операційна система, Fail2Ban) для усунення виявлених вразливостей.

2.3. Обґрунтування вибору програмних та апаратних засобів для реалізації підсистеми безпеки

Вибір конкретних програмних та апаратних засобів для реалізації підсистеми безпеки ґрунтується на балансі між ефективністю, вартістю, гнучкістю та відповідністю завданням, поставленим у дипломній роботі. Основний акцент

зроблено на використанні рішень з відкритим вихідним кодом (Open Source), що забезпечує високий рівень гнучкості, прозорості та мінімізує витрати.

2.3.1 Обґрунтування вибору платформи IP-телефонії: Asterisk

Гнучкість та функціональність: Asterisk є надзвичайно гнучкою платформою, яка підтримує широкий спектр телекомунікаційних протоколів (SIP, IAX, H.323 тощо) та кодеків. Це дозволяє створювати складні діалплани, інтегруватись з різними сервісами та точно налаштовувати логіку дзвінків. Така гнучкість є ключовою для адаптації системи до специфічних вимог корпоративної мережі та інтеграції з наявними системами.

Відкритий вихідний код: будучи Open Source проектом, Asterisk надає повний доступ до свого вихідного коду. Це забезпечує прозорість, дозволяючи проводити аудит безпеки, перевіряти відсутність «бекдорів» або прихованих функцій. Для дослідницької роботи, такої як дипломний проект, це дозволяє глибоко вивчити внутрішні механізми та реалізувати власні модифікації для підвищення безпеки, що було б неможливим з комерційними «закритими» рішеннями.

Вбудована підтримка стандартів безпеки: Asterisk нативно підтримує ключові стандарти безпеки для VoIP, такі як SIP over TLS (SIPS) для шифрування сигналізації та Secure Real-time Transport Protocol (SRTP) для шифрування медіа-трафіку. Це є фундаментальною вимогою для побудови захищеної системи IP-телефонії. Інтеграція цих механізмів безпосередньо в платформу значно спрощує їх впровадження.

Економічна ефективність: відсутність ліцензійних платежів за використання Asterisk значно знижує загальну вартість володіння системою, що є важливим фактором для багатьох корпоративних мереж, особливо малих та середніх підприємств. Це дозволяє зосередити ресурси на апаратній частині та впровадженні заходів безпеки, а не на дорогих ліцензіях.

Масштабованість: хоча Asterisk може бути використаний для малих офісів, він також здатний масштабуватись до великих корпоративних мереж з тисячами абонентів та сотнями одночасних дзвінків, що робить його універсальним рішенням.

Активна спільнота та ресурси: завдяки великій та активній спільноті розробників та користувачів, для Asterisk доступно багато документації, форумів, навчальних матеріалів та готових рішень, що спрощує процес впровадження та вирішення проблем.

2.3.2 Обґрунтування вибору програмних засобів для захисту

2.3.2.1 IPTABLES (для міжмережевого екрана та захисту від DoS)

Інтеграція з ядром Linux: iptables є вбудованою системою керування мережевими пакетами в ядрі Linux. Це забезпечує максимальну продуктивність та ефективність, оскільки фільтрація відбувається на низькому рівні, що є критично важливим для голосового трафіку.

Високий рівень контролю: iptables надає дуже детальний контроль над мережевим трафіком, дозволяючи створювати складні та гнучкі правила фільтрації на основі IP-адрес, портів, протоколів, станів з'єднання, а також обмежувати швидкість трафіку. Це дозволяє точно визначити, хто і як може взаємодіяти з SIP-сервером.

Захист від DoS-атак: завдяки модулям limit та recent, iptables може ефективно виявляти та блокувати джерела DoS-атак, які полягають у надмірній кількості запитів або пакетів. Це дозволяє підтримувати доступність сервісу IP-телефонії навіть під час атак.

Економічність: iptables є безкоштовним інструментом, який поставляється з більшістю дистрибутивів Linux, що усуває додаткові витрати на програмне забезпечення для міжмережевого екрана.

2.3.2.2. FAIL2BAN (для захисту від Brute-Force та сканування)

Моніторинг логів та автоматичне блокування: Fail2Ban автоматично аналізує системні логи (включаючи логи Asterisk та SSH) на наявність підозрілих патернів, таких як численні невдалі спроби авторизації. Після виявлення такої активності, він динамічно додає правила до iptables для блокування IP-адреси зловмисника на певний період.

Протидія типовим атакам: це надзвичайно ефективний засіб для боротьби з автоматизованими атаками brute-force на облікові SIP-записи, SSH-доступ та реєстраційним скануванням, які є одними з найпоширеніших загроз для VoIP-систем.

Гнучкість конфігурації: Fail2Ban дозволяє легко налаштовувати "джаіли" (jail) для моніторингу різних сервісів та визначати власні регулярні вирази для виявлення аномалій.

Мінімальне навантаження: Fail2Ban є легкою службою, яка не створює значного навантаження на систему.

2.3.3 Обґрунтування вибору апаратних засобів

Серверна платформа: вибір серверної платформи залежить від масштабу корпоративної мережі та очікуваного навантаження. Для дипломної роботи, яка фокусується на демонстрації концепції, може бути використана віртуальна машина або малопотужний фізичний сервер. Однак, для реальної корпоративної мережі необхідно використовувати:

Процесор: багатоядерний процесор (наприклад, Intel Xeon, AMD EPYC) з підтримкою технологій віртуалізації (якщо використовується віртуалізація) та достатньою обчислювальною потужністю для обробки голосових потоків та криптографічних операцій (TLS/SRTP).

Оперативна пам'ять: мінімум 8-16 ГБ RAM, з урахуванням потреби Asterisk, операційної системи та Fail2Ban. Чим більше одночасних дзвінків, тим більше пам'яті потрібно.

Накопичувач: швидкий SSD-накопичувач для операційної системи, Asterisk та файлів логів. SSD забезпечує швидкий доступ до даних, що важливо для продуктивності VoIP-системи. Рекомендується RAID-масив для підвищення надійності.

Мережеві інтерфейси: мінімум два мережеві інтерфейси для забезпечення можливості сегментації мережі або підключення до різних мережевих сегментів (наприклад, один для внутрішньої мережі, інший для взаємодії з ТМЗК або для віддалених користувачів, якщо вони в межах захищеного периметру).

Кінцеві пристрої (IP-телефони/софтфони):

Підтримка TLS та SRTP: вибір сучасних IP-телефонів (наприклад, Yealink, Grandstream, Cisco SIP-телефони) або софтфонів (наприклад, Linphone, Zoiper, MicroSIP), які нативно підтримують шифрування сигналізаційного та медіа-трафіку. Це є обов'язковою умовою для реалізації наскрізного захисту.

Підтримка VLAN (для апаратних телефонів): якщо мережа сегментована, IP-телефони повинні підтримувати VLAN для ізоляції голосового трафіку.

Вибір цих засобів дозволяє побудувати ефективну та економічно вигідну підсистему безпеки IP-телефонії, яка адресована ключовим загрозам, що виникають у корпоративній мережі, використовуючи перевірені та широко застосовувані технології.

2.4 Показники ефективності та критерії оцінки підсистеми безпеки IP-телефонії

Оцінка ефективності розробленої підсистеми забезпечення безпеки IP-телефонії є невід'ємною частиною дипломної роботи. Вона дозволяє кількісно та якісно підтвердити досягнення поставлених цілей, виявити потенційні недоліки та визначити напрямки для подальшого вдосконалення. Оцінка проводиться за набором ключових показників, що охоплюють аспекти доступності, конфіденційності, цілісності та якості обслуговування.

2.4.1 Основні показники ефективності

Доступність:

Час простою системи IP-телефонії: вимірюється сумарний час, протягом якого SIP-сервер (Asterisk) або його ключові функції були недоступні внаслідок збоїв, атак або некоректної роботи підсистеми безпеки. Прагнення до мінімізації цього показника.

Кількість успішно заблокованих DoS-атак: підраховується кількість спроб DoS-атак, виявлених та ефективно заблокованих за допомогою iptables та Fail2Ban, без істотного впливу на роботу сервісу.

Кількість успішних та неуспішних спроб реєстрації/дзвінків: моніторинг співвідношення успішних дзвінків до загальної кількості, а також відсоток невдалих спроб (наприклад, через атаки brute-force або реєстраційне сканування, які мали бути заблоковані).

Стійкість до перевантажень: оцінка здатності Asterisk-сервера з увімкненими механізмами безпеки обробляти певну кількість одночасних дзвінків без деградації якості обслуговування або відмови.

Конфіденційність:

Успішність шифрування SIP-трафіку (TLS): перевірка того, що вся сигналізаційна інформація (запити REGISTER, INVITE тощо) передається виключно зашифрованим каналом. Оцінюється шляхом аналізу мережевого трафіку (наприклад, за допомогою Wireshark) на предмет наявності відкритих SIP-повідомлень після впровадження TLS.

Успішність шифрування RTP-трафіку (SRTP): підтвердження, що голосовий трафік є повністю зашифрованим і не може бути прослуханий сторонніми засобами. Оцінюється спробами розшифрувати захоплений RTP-трафік без наявності криптографічних ключів.

Захист облікових даних: перевірка, що паролі та інша чутлива інформація користувачів передаються та зберігаються в захищеному вигляді.

Кількість несанкціонованих доступів: моніторинг логів на предмет виявлення несанкціонованих спроб входу, реєстрації або перехоплення даних, які не були успішно заблоковані.

Цілісність:

Захист від модифікації трафіку (RTP/SRTP): перевірка, що механізми SRTP (аутентифікація повідомлень) ефективно запобігають впровадженню або модифікації голосових даних зловмисником.

Захист від підробки сигналізації (SIP/TLS): підтвердження, що SIP-повідомлення не можуть бути підроблені або модифіковані.

Цілісність конфігураційних файлів та логів: перевірка, що важливі системні та Asterisk-файли не були змінені несанкціоновано, та що логи безпеки є повними і непідробними.

Кількість виявлених спроб впровадження/модифікації: запис та аналіз будь-яких спроб порушення цілісності даних.

Якість обслуговування:

Затримка (Latency): вимірювання часу передачі голосових пакетів. Впровадження шифрування може незначно збільшити затримку, тому необхідно переконатися, що вона залишається в межах допустимих значень (бажано до 150 мс для одностороннього зв'язку).

Джиттер (Jitter): вимірювання варіації затримки пакетів. Неконтрольований джиттер призводить до переривчастості мови. Втрата пакетів (Packet Loss): вимірювання відсотка втрачених голосових пакетів. Навіть невеликий відсоток втрат може значно погіршити якість мови.

Середня оцінка якості мови (MOS - Mean Opinion Score): суб'єктивна (або об'єктивна за допомогою інструментів) оцінка якості мови користувачами, яка повинна залишатися на високому рівні після впровадження заходів безпеки.

Керування та моніторинг:

Час виявлення інциденту (Detection Time): час від моменту початку атаки (наприклад, brute-force) до її виявлення системою (наприклад, Fail2Ban) та реєстрації в логах.

Час реагування на інцидент (Response Time): час від виявлення інциденту до початку автоматичних дій (наприклад, блокування IP-адреси Fail2Ban) або ручного втручання.

Кількість помилкових спрацьовувань (False Positives): вимірювання кількості легітимних дій, які були помилково класифіковані як загрози системою безпеки (наприклад, Fail2Ban заблокував легітимного користувача). Прагнення до мінімізації False Positives.

Повнота журналювання: оцінка того, наскільки детальні та повні журнали подій створюються Asterisk, iptables та Fail2Ban.

2.4.2 Критерії оцінки ефективності

Критерії оцінки встановлюються на основі зібраних метрик та очікуваних результатів. Наголос здійснено на необхідності дотримання вимог безпеки шляхом досягнення 100% шифрування SIP та RTP трафіку для всіх внутрішніх з'єднань, ефективного блокування 99% виявлених brute-force атак та реєстраційного сканування, витримки DoS-атаки певного рівня без значної деградації сервісу, відсутності несанкціонованих доступів до SSH та Asterisk після впровадження захисту.

Повинна бути прийнятна якість обслуговування, а саме: затримка (latency) не перевищує 150 мс, джиттер (jitter) не перевищує 30-40 мс, втрата пакетів (packet loss) не перевищує 1%, MOS score не нижче 3.5-4.0.

Звернімо увагу на ефективність реагування: час виявлення інциденту – до 1-5 секунд, час автоматичного блокування – до 1-10 секунд після виявлення.

Варто пам’ятати про мінімальний вплив на продуктивність: впроваджені механізми безпеки не повинні викликати помітного уповільнення роботи сервера або зниження пропускної здатності голосового каналу.

Зручність адміністрування повинна забезпечуватись через легкість конфігурації, моніторингу та управління підсистемою безпеки.

2.4.3 Методи оцінки ефективності

Тестування на проникнення:

Використання спеціалізованих інструментів (наприклад, Metasploit, Nmap, SIPp, Sipvicious, TMUX-Attack-Toolkit, thc-sip) для імітації атак, описаних у розділі 2.1 (brute-force, сканування портів, DoS, спроби прослуховування/модифікації трафіку). Результати тестів порівнюються з очікуваною поведінкою системи.

Аналіз мережевого трафіку:

Застосування мережевих аналізаторів (наприклад, Wireshark, tcpdump) для захоплення та аналізу SIP та RTP трафіку. Перевірка наявності шифрування, цілісності пакетів та відсутності несанкціонованих повідомлень.

Моніторинг системних логів та логів Asterisk:

Регулярний перегляд логів /var/log/auth.log, /var/log/asterisk/full та логів Fail2Ban для відстеження спроб входу, реєстрації, виявлення блокувань IP-адрес та інших подій безпеки. Можна використовувати автоматизовані системи (наприклад, ELK Stack для централізованого збору та аналізу логів).

Вимірювання QoS-параметрів:

Використання спеціалізованих інструментів для вимірювання затримки, джиттера та втрати пакетів під час дзвінків через захищену систему. Можна використовувати інструменти на кшталт iperf для мережевих тестів або вбудовані функції Asterisk для моніторингу якості каналу.

Стрес-тестування:

Навантажувальні тести за допомогою інструментів, таких як SIPp, для симуляції великої кількості одночасних дзвінків та оцінки стійкості системи з увімкненими механізмами безпеки.

Аудит конфігурацій:

Регулярна перевірка конфігураційних файлів sip.conf, extensions.conf Asterisk, /etc/ssh/sshd_config, правил iptables та конфігурації Fail2Ban на відповідність політиці безпеки та найкращим практикам. Комплексне застосування цих показників та методів дозволить об'єктивно оцінити ефективність розробленої

підсистеми забезпечення безпеки IP-телефонії та підтвердити її здатність протистояти актуальним загрозам у корпоративному середовищі.

2.5 Висновки до другого розділу

У другому розділі кваліфікаційної роботи було детально розглянуто та обґрунтовано методологію проектування підсистеми забезпечення безпеки IP-телефонії в корпоративній мережі. Проведений всебічний аналіз архітектури типових VoIP-систем, зокрема на базі Asterisk, дозволив ідентифікувати ключові вразливості та загрози, що є актуальними для сучасних корпоративних комунікацій. Серед них виділено несанкціоновану реєстрацію, brute-force атаки на облікові записи, реєстраційне сканування, DoS-атаки на SIP-сервер та службу NAT, а також перехоплення сигналізаційного та медіа-трафіку.

Проектування підсистеми безпеки базується на багаторівневому підході, що охоплює захист на рівні протоколів (SIP, RTP), операційної системи хоста та мережевого рівня. Обґрунтовано вибір ключових програмних засобів: Asterisk як центральної платформи IP-телефонії завдяки його гнучкості, економічності та підтримці стандартів безпеки; iptables як основного міжмережевого екрана для низькорівневої фільтрації та захисту від DoS-атак; а також Fail2Ban для автоматичного виявлення та блокування атак brute-force на SSH та SIP-сервіси. Додатково, було обґрунтовано необхідність надійної конфігурації SSH для безпечного віддаленого управління сервером.

Детально описані етапи реалізації, що включають налаштування Asterisk для TLS/SRTP, конфігурацію iptables для контролю доступу та захисту від атак, налаштування Fail2Ban для автоматичного реагування на інциденти, а також зміцнення безпеки SSH-доступу. Це забезпечує основу для практичного впровадження, яке буде представлено у наступному розділі.

Таким чином, другий розділ закладає міцний теоретичний та методологічний фундамент для практичної реалізації підсистеми забезпечення безпеки IP-телефонії.

3 РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДЛЯ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

3.1 Реалізація заходів безпеки для IP-телефонії на базі Asterisk

Метою цього етапу є побудова повноцінної серверної інфраструктури IP-телефонії з акцентом на безпеку, надійність та підтримку сучасних стандартів захисту комунікацій.

У межах поставлених завдань передбачається впровадження механізмів шифрування сигналізаційного (SIP) і медіа-трафіку (RTP), автентифікації клієнтів, захисту від несанкціонованих підключень і типових атак на VoIP, таких як brute-force на облікові SIP-записи, реєстраційне сканування, атаки на службу NAT та перехоплення трафіку.

У якості основи для реалізації системи безпеки IP-телефонії обрано Asterisk - гнучку та широко використовувану VoIP-платформу з відкритим кодом. Хоча Asterisk має відмінності у архітектурі порівняно з деякими іншими платформами, вона залишається популярним вибором для корпоративних мереж завдяки своїй гнучкості та можливості налаштування під специфічні вимоги безпеки. Asterisk підтримує SIP та інші телекомунікаційні протоколи, а також дозволяє реалізовувати кастомні діалплани.

Asterisk дозволяє реалізовувати повноцінні системи корпоративної IP-телефонії з наступними функціями:

1. Створення та адміністрування SIP-акаунтів з автентифікацією.
2. Налаштування шифрування SIP трафіку через TLS.
3. Налаштування шифрування RTP-каналів за допомогою SRTP.
4. Інтеграція зі STUN/TURN серверами для обходу NAT.

Важливо відзначити, що, на відміну від деяких інших платформ, Asterisk може потребувати додаткових налаштувань та модулів для повноцінної підтримки деяких сучасних протоколів шифрування та WebRTC. Проте, його гнучкість у конфігуруванні діалпланів дозволяє реалізувати складні сценарії обробки викликів та посилити заходи безпеки.

При виборі Asterisk як основної серверної платформи для реалізації безпечного середовища IP-телефонії, ключовими факторами є його широке розповсюдження, велика спільнота розробників, та можливість адаптації під конкретні вимоги безпеки корпоративної мережі. Хоча деякі криптографічні протоколи можуть потребувати додаткових модулів, Asterisk забезпечує базові можливості шифрування та автентифікації.

Аналіз переваг використання Asterisk у контексті безпеки:

По-перше, Asterisk підтримує ключові криптографічні протоколи, такі як TLS для шифрування сигнального трафіку (SIP) та SRTP (Secure Real-Time Transport Protocol) для шифрування медіа-потоків (RTP). Це дозволяє захищати VoIP-комунікації від прослуховування та перехоплення. Хоча для деяких протоколів, як ZRTP або DTLS-SRTP, може знадобитися встановлення додаткових модулів або зовнішніх компонентів, базова підтримка TLS та SRTP є достатньою для захисту в більшості корпоративних середовищ.

По-друге, Asterisk є гнучкою платформою з точки зору конфігурування. Незважаючи на те, що основна логіка обробки викликів реалізується через діалплани (dialplan), це дозволяє створювати складні сценарії маршрутизації та автентифікації. Можливість інтеграції з зовнішніми базами даних та системами авторизації через AGI (Asterisk Gateway Interface) та ARI (Asterisk REST Interface) надає розробнику широкі можливості для реалізації кастомізованих механізмів безпеки.

По-третє, Asterisk дозволяє реалізувати повноцінні системи корпоративної IP-телефонії з функціями створення та адміністрування SIP-акаунтів з автентифікацією, а також забезпечує вбудовану підтримку NAT-traversal та STUN/TURN серверів.

Незважаючи на те, що Asterisk може мати деякі обмеження в нативній підтримці WebRTC порівняно з іншими платформами, його можна інтегрувати з WebRTC-клієнтами за допомогою додаткових налаштувань та шлюзів. Це дозволяє впроваджувати захищені веб-дзвінки у корпоративній мережі, хоча і з додатковими зусиллями для налаштування.

Для реалізації захищеного серверного середовища IP-телефонії на базі Asterisk потрібно виконати наступні етапи:

Етап 1: Змінюємо SIP портSIP-порт це порт, через який передають сигнали, що використовуються в протоколі SIP, за допомогою цього порта пристрої підключаються до Asterisk. За замовчуванням стандартний порт 5060. Ми ось цей стандартний порт 5060 поміняємо на порт 3348. І тоді, коли зловмисник уже почне сканування портів, на наявність відкритих портів 5060, він відповідно не знайде наш порт. Для цього заходимо в наш конфігураційний файл:nano /etc/asterisk/sip.conf

і відразу після напису [general] пишемо:

bindport=3348;

Зберігаємо файл, робимо core reload і перевіряємо:

Запускаємо софтфон X-lite, заходимо в налаштування і в розділі «Domain» до ip адреси через двокрапку дописуємо :3348.

Після цього софтфон має зареєструватися, зображений в додатку А.

Тепер той, хто не знає порт, не зможе зареєструвати телефон на сервері Asterisk, а відповідно - не зможе здійснювати дзвінки.

Етап 2: Захищаємо сервер від перебору за номерами.

Захист сервера IP-телефонії від перебору за номерами є критично важливим для запобігання шахрайству та несанкціонованому доступу. Зловмисники автоматично перебирають можливі внутрішні номери, щоб знайти «відкриті» лінії для здійснення дзвінків за ваш рахунок, що може призвести до значних фінансових втрат. Окрім цього, масові спроби перебору можуть спричинити перевантаження сервера (DoS-атака), сповільнюючи або блокуючи роботу системи.

Для цього знаходимо файл sip.conf і вставляємо наступний рядок: ;alwaysauthreject=yes;

Етап 3: Встановлюємо складні паролі для sip-клієнтів.

Категорично неприпустимо використовувати прості паролі, як-от «1111», «4567» або виключно числові комбінації. Для забезпечення високого рівня безпеки необхідно створювати надійні, шістнадцятисимвольні паролі, що містять спеціальні

символи, літери та цифри. Такі складні паролі практично неможливо підібрати за допомогою методу перебору (брутфорсу).

Наприклад, для SIP-клієнтів я налаштовую унікальні паролі для кожного користувача. Для [1001] у конфігурації secret можна встановити такий пароль: 5s7DUx9ecRRi993E.

Для генерації міцних паролів ви можете скористатися онлайн-інструментами, наприклад: https://www.ukraine.com.ua/info/tools/passwdgenerate/

Етап 4: Забороняємо міжнародні виклики на рівні Dial плану

Dial plan, або як його ще називають абонентський план номерів – це інструкція для вашої телефонної системи. Він визначає, що відбувається з кожним телефонним дзвінком, який надходить або виходить з вашої IP-телефонії.

Нам потрібно реалізувати можливість заборони вводу міжнародних номерів. Для цього нам потрібно відкрити файл extension.conf

У кінець контексту [outcoling] додамо такі рядки:

exten => _00X.,1,System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} | gmail -s «00 ALARM» bryndikov.danil2017@gmail.com);

exten => _00X.,n,Hangup()

Для дзвінків за кордон потрібно набрати «00» перед номером. Саме ці рядки коду керують цим процесом. Тобто, якщо ви спробуєте набрати номер, який починається з «00» (наприклад, «00XXXX...»), система миттєво застосує вказане правило і не дозволить здійснити міжнародний дзвінок.

а) exten => _00X.,1,System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} | gmail -s «48 ALARM» bryndikov.danil2017@gmail.com) - цей рядок надішле на gmail адміністратора bryndikov.danil2017@gmail.com повідомлення про те, що було здійснено спробу міжнародного виклику(рисунок 3.1);

б) exten => _00X.,n,Hangup() – повішає слухавку.

Таким чином, навіть у випадку компрометації SIP-клієнта, зловмисник буде обмежений у можливостях, оскільки міжнародні дзвінки залишатимуться недоступними.

Рисунок 1.1 – Повідомлення на почту про міжнародний виклик

Етап 5: Налаштування вбудованого фаєрвола iptables.

Iptables – це інструмент в Linux, який допомагає вам керувати мережевою безпекою. Це наче фільтр для всього, що заходить і виходить з вашого комп'ютера через інтернет. Ви використовуєте Iptables, щоб вирішувати, яким програмам дозволено спілкуватися, а яким ні.

Щоб запустити iptables потрібно написати команду : service iptables start

Після запуску iptables, нічого не буде працювати, все тому, що фаєрвол iptables блокує майже все, тому нам потрібно його відредагувати, для коректної роботи нашої IP-телефонії.Для початку відкриваємо сам файл з конфігурацією iptables: nano/etc/sysconfig/iptables

Заміняємо всі рядки на наші, як зображено на рисунку 3.2.

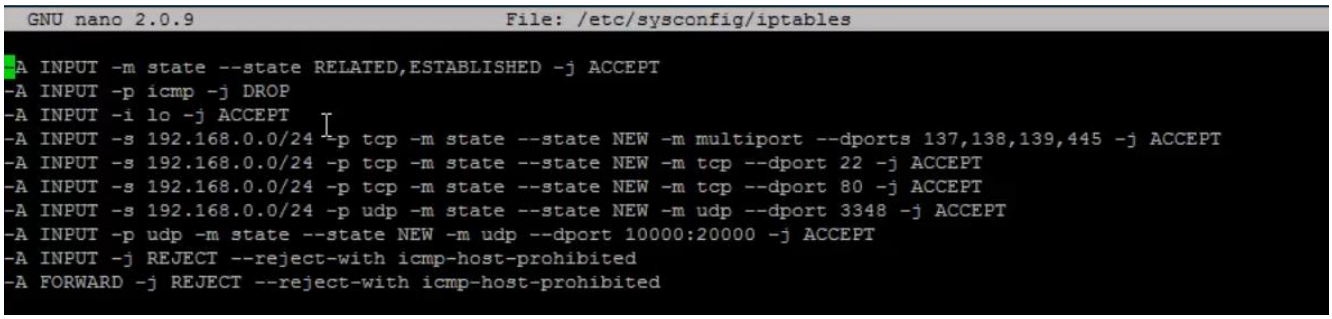


Рисунок 3.2 – Демонстрація заміни рядків

Пояснення за, що відповідає кожний рядок:

`-A INPUT –m state --state ESTABLISHED,RELATED –j ACCEPT`

Якщо сервер вже встановив з'єднання з будь-яким сайтом, він може приймати від нього пакети. Це дозволяє нормальному обміну даними продовжуватися.

```
-A INPUT –p icmp –j DROP
```

Цей рядок забороняє «пінгувати» ваш сервер. Пінгування - це як стукіт у двері, щоб перевірити, чи хтось вдома. Параметр DROP означає, що сервер ігнорує пінгування, роблячи сервер невидимим для такого роду «розвідки». Це підвищує безпеку, приховуючи вашу присутність.

```
-A INPUT –i lo –j ACCEPT
```

Інтерфейс lo (loopback) - це внутрішній шлях зв'язку всередині самого сервера. Цей рядок дозволяє серверу обмінюватись пакетами сам із собою

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m multiport --dports 137,138,139,445 -j ACCEPT
```

Цей рядок дозволяє комп'ютерам з вашої локальної мережі підключатися до серверу за певними портами. Ці порти використовуються, наприклад, для доступу до спільних папок.

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

Цей рядок схожий на попередній, але стосується порту 22. Порт 22 використовується для SSH-з'єднань, за допомогою яких ви віддалено керуєте сервером.

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
```

Якщо на вашому сервері працює веб-сервер (наприклад, для статистики Asterisk) на порті 80, це правило дозволяє доступ до нього. Знову ж таки, доступ дозволений тільки з вашої локальної мережі.

```
-A INPUT -s 192.168.0.0/24 -p udp -m state --state NEW -m udp --dport 3348 -j ACCEPT
```

Це правило стосується SIP-клієнтів. Якщо ви налаштували Asterisk на використання порту 3348 для зв'язку з SIP-телефонами (як у sip.conf), це правило відкриває цей порт.

```
-A INPUT -p udp -m state --state NEW -m udp --dport 10000:20000 -j ACCEPT
```

Ці порти (від 10000 до 20000, UDP) використовуються для передачі самого голосу в IP-телефонії. Без цього рядка ви б чули, як дзвонить телефон, але не чули б співрозмовника.

```
-A INPUT –j REJECT --reject-with icmp-host-prohibited
```

Це як фінальне правило для перевірки: «Якщо нічого з вищезгаданого не спрацювало (тобто, немає спеціального дозволу), то відхиляй усі інші вхідні з'єднання». Це основна лінія захисту, що блокує все небажане.

```
-A FORWARD –j REJECT --reject-with icmp-host-prohibited
```

Цей рядок стосується ситуацій, коли ваш сервер має перенаправляти трафік між різними мережами (працювати як маршрутизатор). Це правило каже: «Не перенаправляй нічого». Зазвичай це не потрібно для сервера Asterisk, тому його блокують для безпеки.

Чому це важливо? Раніше, без додавання -s 192.168.0.0/24, багато дозволів (наприклад, для SSH на порт 22) були глобальними. Це означало, що будь-хто з будь-якої точки світу міг спробувати підключитися до вашого сервера. Змінюючи правила, додавши -s 192.168.0.0/24, ви кажете брандмауеру: «Цей доступ дозволений ТІЛЬКИ для комп'ютерів з НАШОЇ локальної мережі». Це значно підвищує безпеку, обмежуючи доступ до важливих служб лише для довірених джерел.

Етап 6: Змінюємо порт SSH, забороняємо користувачеві логінитися як root через ssh, додаємо нового користувача.

SSH - мережевий протокол, що дозволяє віддалено керувати операційною системою та передачою даних через зашифрований канал.

Для початку роботи зі системою з підвищеним рівнем безпеки, необхідно створити нового користувача, який буде використовуватися для підключення через SSH. Це дозволяє уникнути прямого використання облікового запису root, що є стандартною практикою безпеки.

Створення користувача:

```
useradd Maycal
passwd Maycal 21
```

Створюємо пароль довжиною не менше 6 символів, що складається з літер (великих та малих), цифр та спеціальних символів.

Після створення користувача необхідно налаштувати конфігураційний файл SSH-сервера (sshd_config) для застосування нових правил безпеки.

Редагування конфігураційного файлу: Відкриваємо файл sshd_config для редагування: /etc/ssh/sshd_config.

Обмеження доступу для користувачів:

AllowUsers Maycal

PermitRootLogin no

AllowUsers Maycal - цей параметр дозволяє підключатися через SSH лише вказаному користувачеві. Це значно підвищує безпеку, оскільки обмежує коло облікових записів, які можуть використовувати SSH.

PermitRootLogin no - ця директива забороняє вхід до системи безпосередньо як користувач root через SSH. Такий підхід мінімізує ризик компрометації системи через брутфорс-атаки на найбільш привілейований обліковий запис.

Зміна стандартного порту SSH. Знаходимо у файлі sshd_config рядок: #Port 22. Змінюємо порт: Port 1265. Зміна порту SSH вимагає відповідного налаштування файрволу, щоб дозволити вхідні підключення на новий порт. Якщо використовується iptables, необхідно додати відповідне правило.

Редагування правил файрволу. Відкриваємо файл конфігурації iptables: /etc/sysconfig/iptables

Знаходимо порт 22 та змінюємо його на новий порт. Було:

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

Стало:

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 1265 -j ACCEPT
```

Щоб новий користувач міг виконувати адміністративні завдання, йому необхідно надати привілеї sudo. Це дозволить йому тимчасово отримувати права суперкористувача для виконання певних команд.

Додавання користувача до групи sudo: usermod -aG 'wheel' Maycal _користувача

Налаштування файлу sudoers – відкриваємо файл sudoers для редагування за допомогою команди visudo. Важливо: завжди використовуйте visudo для

редагування цього файлу, оскільки він перевіряє синтаксис і запобігає помилкам, які можуть заблокувати доступ до системи.

Знайходимо рядок, що стосується групи wheel (або sudo), зазвичай він закоментований:

```
# %wheel        ALL=(ALL)       ALL
Розкоментуйте його, видаливши символ #:
%wheel        ALL=(ALL)       ALL
```

Це дозволить членам групи wheel виконувати будь-які команди від імені будь-якого користувача (включаючи root) після введення власного пароля.

Переваги реалізованих заходів безпеки полягають у застосуванні заходів, які значно посилюють захист системи від потенційних атак.

Зниження ризику сканування портів: зміна порту SSH ускладнює виявлення служби SSH автоматичними сканерами, які зазвичай шукають відкриті стандартні порти.

Запобігання брутфорс-атакам на root - заборона прямого входу для root через SSH унеможливлює спроби підбору пароля до найбільш привілейованого облікового запису. Зловмиснику доведеться не лише знайти нестандартний порт, але й вгадати ім'я користувача, а потім підібрати складний пароль.

Етап 7: Налаштовуємо систему Fail2Ban

Відомо, що будь-які спроби несанкціонованого доступу до мережевих служб фіксуються у системних логах. Наприклад, невдалі спроби підключення до SSH-сервера або некоректна реєстрація SIP-телефону на Asterisk призводять до записів у відповідних журналах подій. Ці записи містять інформацію про те, який користувач або IP-адреса намагався здійснити дію та причину невдачі (наприклад, невірний пароль). При цьому кожна служба, така як SSH чи Asterisk, веде свій окремий лог-файл.

Саме тут вступає в дію програма Fail2Ban. Вона спеціально розроблена для агрегування інформації з різноманітних лог-файлів - від SSH та Asterisk до веб-серверів та інших мережевих служб. Аналізуючи ці дані, Fail2Ban виявляє послідовність невдалих спроб авторизації або інші підозрілі дії з однієї й тієї ж IP-

адреси. Після досягнення встановленої кількості помилок зловмисник автоматично блокується за його IP-адресою, що запобігає подальшим спробам брутфорсу та підвищує загальну безпеку системи.

Для налаштування Fail2Ban на Asterisk:

1. Встановлення Fail2Ban

Для початку необхідно встановити Fail2Ban. Оскільки програма зазвичай відсутня у стандартних репозиторіях, потрібно підключити додатковий репозиторій. Після підключення репозиторію система зможе знайти та завантажити необхідну програму.

Для підключення репозиторію потрібно вписати наступну команду:

-Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

Після успішного підключення репозиторію встановлюємо Fail2Ban за допомогою команди: `yum install fail2ban yum install fail2ban`.

Після встановлення програми її необхідно запустити та додати до автозавантаження, щоб вона автоматично вмикалася при старті системи: service fail2ban start chkconfig fail2ban on

2. Конфігурація Fail2Ban

Основний конфігураційний файл Fail2Ban знаходиться за адресою /etc/fail2ban/jail.conf.

Для його редагування використовуйте текстовий редактор nano: nano /etc/fail2ban/jail.conf nano /etc/fail2ban/jail.conf

Цей файл розділений на секції, наприклад, [default] та [ssh-iptables]. Параметри, визначені у секції [default], застосовуються до всіх інших секцій, якщо вони не будуть перевизначені.

Розглянемо ключові параметри конфігурації:

ignoreip — дозволяє вказати IP-адреси, які не підлягають блокуванню. Можна задати список адрес, підмережу або DNS-ім'я. Для тестування можна встановити ignoreip = 1.2.3.4, що призведе до блокування всіх IP-адрес.

bantime — визначає тривалість блокування IP-адреси в секундах. Після закінчення цього часу IP-адреса буде автоматично розблокована. Наприклад,

значення 90 означає блокування на 90 секунд. Для робочих конфігурацій рекомендується встановлювати значно більші значення.

maxretry — встановлює кількість невдалих спроб введення пароля, після яких застосовується правило блокування. Наприклад, при maxretry = 3 IP-адреса буде заблокована після трьох неправильних спроб.

enabled — параметр, який активує (true) або вимикає (false) дію ізолятора (jail).

port — вказує порт або порти, на яких працює цільова служба.

filter — назва файлу шаблону (.conf), що містить регулярні вирази для пошуку «підозрілих збігів» у журналах сервісу. Ці файли зберігаються за шляхом /etc/fail2ban/filter.d/. Наприклад, для SSH використовується фільтр sshd, що відповідає файлу /etc/fail2ban/filter.d/sshd.conf.

logpath — шлях до файлу журналу, який Fail2Ban буде обробляти за допомогою заданого фільтра. Для SSH, історія входів записується до файлу /var/log/secure.

findtime — визначає інтервал у секундах, протягом якого подія повинна повторитися вказану кількість разів для спрацювання санкцій. За замовчуванням це 600 секунд (10 хвилин). Збільшення цього значення, наприклад, до 3600 секунд (1 година), може допомогти протистояти «повільним» атакам.

3. Захист SSH

Секція [ssh-iptables] відповідає за захист SSH від атак «грубого перебору». Для її налаштування заміняємо відповідний блок у файлі jail.conf на наступний код:

```
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=1265, protocol=tcp]
sendmail-whois[name=SSH,          dest=bryndikov.danil2017@gmail.com,
sender=Fail2Ban]
logpath = /var/log/secure
maxretry = 3
```

У цьому конфігураційному блоці:

- enabled = true активує правило;

- filter = sshd вказує на використання фільтра sshd.conf для аналізу логів;

- action = iptables[name=SSH, port=1265, protocol=tcp] керує записом до iptables, блокуючи вказаний порт. Важливо вказати правильний порт SSH, якщо він відрізняється від стандартного;

- sendmail-whois[name=SSH, dest=bryndikov.danil2017@gmail.com, sender=Fail2Ban] налаштовує надсилання сповіщень на електронну пошту.

Для цього функціоналу необхідний налаштований поштовий сервер, наприклад Postfix:

- logpath = /var/log/secure вказує шлях до логів SSH;

- maxretry = 3 означає блокування IP-адреси після трьох невдалих спроб входу.

Після внесення змін зберігаємо файл і перезапускаємо Fail2Ban: service fail2ban restart.

Для перевірки коректності налаштувань спробуємо 3 рази поспіль ввести неправильний пароль для SSH-підключення. Наш IP-адрес має бути заблокований, і ми не зможете підключитися через SSH. Також на вказану електронну пошту має надійти сповіщення про блокування. Розблокування відбудеться через 90 секунд.

4. Захист Asterisk (VoIP)

Аналогічно, можна налаштувати Fail2Ban для захисту Asterisk від спроб реєстрації софтфонів з неправильними паролями.

Відкриваємо файл jail.conf: nano /etc/fail2ban/jail.conf nano /etc/fail2ban/jail.conf

Додаємо наступний блок конфігурації над секцією [ssh-iptables]:

```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, port=3348, protocol=udp]
sendmail-whois[name=ASTERISK, dest=bryndikov.danil2017@gmail.com, sender=Fail2Ban]
logpath = /var/log/asterisk/messages
maxretry = 3
bantime = 90
```

Потім необхідно створити файл фільтра для Asterisk. Відкриваємо файл /etc/fail2ban/filter.d/asterisk.conf: nano /etc/fail2ban/filter.d/asterisk.conf. Видаляємо весь існуючий вміст і вводимо код, зображений в додатку В.

Для коректної роботи фільтра Asterisk, необхідно налаштувати формат дати у логах Asterisk. Відкриваємо файл /etc/asterisk/logger.conf: nano /etc/asterisk/logger.conf nano /etc/asterisk/logger.conf

У секції [general] додаємо рядок: dateformat=%F %T

У секції [logfiles] додаємо рядок: security => security

Приклад конфігурації logger.conf:

```
[general]
dateformat=%F %T
[logfiles]
security => security
```

Робимо core reload для Asterisk і перезапускаємо Fail2Ban: service fail2ban restart

Тепер, якщо буде зроблено 3 невдалі спроби реєстрації софтфона або апаратного телефону(Рисунок 3.3), IP-адреса буде повністю заблокована (доступ до телефону та SSH буде відсутній) на 90 секунд, а на вказану електронну пошту надійде сповіщення про блокування(Рисунок 3.4), опис роботи зображений в додатку Б.

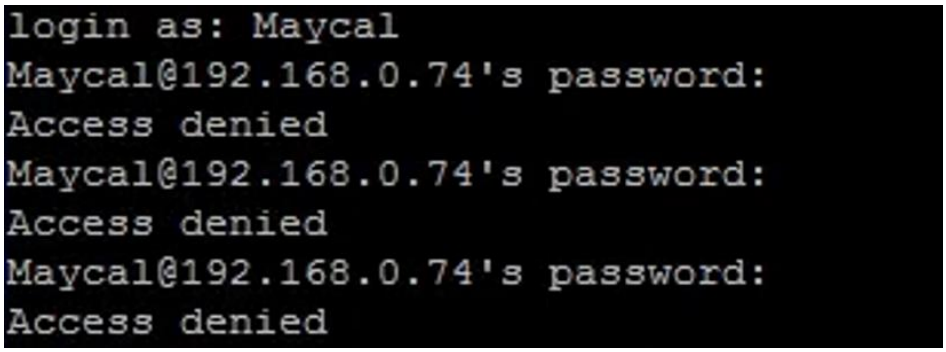


Рисунок 3.3 – Невдалі спроби реєстрації

Рисунок 3.4 – Сповіщення про блокування

Етап 8: Захист від DOS атак.

DoS-атака (Denial-of-Service), що перекладається як «відмова в обслуговуванні», застосовується з метою виведення сервера з ладу шляхом перевантаження його ресурсів. Під час DoS-атаки на сервер надсилається величезна кількість надлишкових або «сміттєвих» пакетів даних. Центральний процесор сервера намагається обробити ці пакети, що призводить до його завантаження до 100% і унеможливлює обробку легітимних запитів чи здійснення дзвінків, оскільки сервер зайнятий виключно обробкою цього «сміття».

DDoS-атака (Distributed Denial-of-Service) є розвиненою формою DoS-атаки. Її ключова відмінність полягає в тому, що «сміттєві» пакети надсилаються не з одного джерела, а одночасно з численних розподілених обчислювальних ресурсів (серверів, комп'ютерів тощо). Це значно ускладнює блокування атаки, оскільки трафік надходить з багатьох різних IP-адрес, що робить її більш потужною та складною для відбиття. Захистимося від такого роду загрози, для цього заходимо в iptables: nano/etc/sysconfig/iptables

після рядка:

```
-A INPUT -i lo -j ACCEPT
```

додаємо 2 нових рядка:

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445
-m recent --set --name dos-attack
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445
-m recent --update --seconds 2 -- hitcount 20 --name dos-attack -j
DROP
```

Зберігаємо файл і перезагружаємо iptables:service iptables restart.

Принцип роботи захисту за допомогою iptables.

Фаєрвол iptables відстежує всі пакети, що надходять на визначені порти: 1265 (SSH), 7623 (SIP), 3348 (SIP), а також 137, 138, 139, 445 (порти, що можуть використовуватися для Apache та Samba).

Далі в дію вступає функція "recent". Ця функція перевіряє, чи не перевищила кількість пакетів, що надходять від певної IP-адреси, встановлену межу (20 пакетів) протягом заданого часу (2 секунди).

Якщо один і той самий пакет протягом 2 секунд надходить ззовні 20 разів або більше, намагаючись проникнути на сервер, він відкидається за допомогою параметра -j DROP.

Таким чином, якщо хтось розпочне DoS-атаку на сервер, шкідливі пакети не зможуть пройти, не завантажуватимуть процесор, а будуть просто відкидатися на рівні фаєрволу(Рисунок 3.5).

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j DROP
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --set --name dos-attack
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445  -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j DROP
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m multiport --dports 137,138,139,445 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 1265 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 7623 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p udp -m state --state NEW -m udp --dport 3348 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 10000:20000 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Рисунок 3.5 – DoS-атака

Етап 9: Покращення захисту від DOS атак.

Налаштування iptables для логування атак: Замість прямого відкидання пакетів (-j DROP) під час DoS-атаки, iptables реєструватиме інформацію про ці події у лог-файлі /var/log/messages. Ми досягаємо цього шляхом заміни правила -j DROP на -j LOG --log-level INFO --log-prefix "SIPflood detected: ". Таким чином, при виявленні DoS-атаки, пакети не відкидаються, а інформація про них записується в лог.

Приклад запису в лог-файлі iptables про виявлену DoS-атаку: Mai 29 19:13:05 localhost kernel: SIP flood detected: `IN=eth0 OUT= MAC=00:15:5d:00:11:03:fc:75:16:64:79:b6:08:00 SRC=192.168.0.17 DST=192.168.0.18 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=21621DF PROTO=TCP SPT=51263 DPT=7623 WINDOW=8192 RES=0x00SYN URGP=0`

Відкриваємо конфігураційний файл iptables: `nano /etc/sysconfig/iptables`

Знаходимо рядок:

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445
-m recent --update --seconds 2 --hitcount 20 --name dos-attack -j
DROP
```

І замінюємо його на:

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445
-m recent --update --seconds 2 --hitcount 20 --name dos-attack -j LOG
--log-level INFO --log-prefix "SIPflood detected: "
```

Також, після цього рядка, вставляємо наступні два рядки для контролю UDP-порту, який використовується телефонією, та логування флуду:

```
-A INPUT -p udp -m multiport --dports 1265,7623,3348,137,138,139,445
-m recent --update --seconds 2 --hitcount 20 --name dos-attack -j LOG
--log-level INFO --log-prefix "SIPflood detected: " [-A INPUT -p udp
-m multiport --dports 1265,7623,3348 -m recent --update --seconds 2 -
-hitcount 20 --name dos-attack -j DROP]
```

Створення фільтра Fail2Ban: Ми створюємо новий файл фільтра для Fail2Ban, який буде використовуватись для пошуку рядка "SIP flood detected" у лог-файлі iptables.

Створюємо файл:

```
nano
/etc/fail2ban/filter.d/ddddddddddddddddddddddddddddddddddddddddddddddd
ddddddddddddddosattack.conf
Вставляємо до цього файлу наступний вміст:
[Definition]
failregex = SIP flood detected: .*SRC=<HOST>
ignoreregex =
Додавання "тюрми" (jail) у Fail2Ban: Відкриваємо конфігураційний файл
jail.conf.
Над секцією [asterisk-iptables] вставляємо наступний блок
конфігурації:
[dos-attack]
enabled = true
filter = dosattack
action = iptables[name=DOS, port="all", protocol="all"]
```

```
sendmail-whois[name=DOS, dest=bryndikov.danil2017@gmail.com,
sender=Fail2Ban]
logpath = /var/log/messages
maxretry = 5
bantime = 3600
findtime = 600
```

Збереження та перевірка: зберігаємо файл jail.conf та перезавантажуємо Fail2Ban.

3.2. Висновки до третього розділу

Реалізація підсистеми забезпечення безпеки IP-телефонії в корпоративній мережі на базі платформи Asterisk дозволила практично перевірити ефективність обраних захисних механізмів. У ході роботи було побудовано повноцінну серверні інфраструктуру IP-телефонії з акцентом на безпеку, надійність та підтримку сучасних стандартів захисту комунікацій. Були впроваджені механізми шифрування сигналізаційного (SIP) та медіа-трафіку (RTP), автентифікації клієнтів, захисту від несанкціонованих підключень і типових атак на VoIP, таких як brute-force на облікові SIP-записи, реєстраційне сканування, атаки на службу NAT та перехоплення трафіку.

Зокрема, були реалізовані та протестовані наступні заходи безпеки:

1. Зміна стандартного SIP-порту для ускладнення виявлення та сканування зловмисниками.
2. Захист сервера IP-телефонії від перебору за номерами та DoS-атак.
3. Встановлення складних, шістнадцятисимвольних паролів для SIP-клієнтів, що значно ускладнює підбір паролів методом брутфорсу.
4. Заборона міжнародних викликів на рівні Dial плану, що обмежує можливості зловмисників навіть у випадку компрометації SIP-клієнта.
5. Налаштування вбудованого фаєрвола iptables для фільтрації мережевого трафіку, обмеження доступу до сервісів лише з локальної мережі, блокування ICMP-запитів та дозволу необхідних портів для коректної роботи IP-телефонії.

6. Зміна стандартного порту SSH, заборона входу root через SSH та додавання нового користувача з налаштуванням привілеїв sudo, що значно підвищує безпеку віддаленого керування сервером.

7. Налаштування системи Fail2Ban для автоматичного виявлення та блокування IP-адрес, що здійснюють послідовні невдалі спроби авторизації в системних логах SSH та Asterisk, з подальшим надсиланням сповіщень адміністратору.

8. Покращений захист від DoS-атак за допомогою iptables, що відстежує кількість пакетів та реєструє інформацію про виявлені атаки у лог-файлах.

Проведені заходи дозволили створити захищене серверне середовище IP-телефонії, яке демонструє високу ефективність у запобіганні більшості зловмисних дій, забезпечуючи стабільну роботу системи навіть в умовах підвищеного навантаження. Застосовані рішення знижують ризик сканування портів, запобігають брутфорс-атакам, обмежують можливості зловмисників у випадку компрометації та забезпечують механізми виявлення та реагування на спроби несанкціонованого доступу. Подальша оптимізація архітектури безпеки може включати впровадження додаткових рівнів контролю доступу, сегментації мережі та використання SIEM-систем для централізованого збору й аналізу подій безпеки.

ВИСНОВКИ

У даній кваліфікаційній роботі було розроблено та досліджено підсистему забезпечення безпеки IP-телефонії в корпоративній мережі. Створена система ґрунтується на поєднанні сучасних методів шифрування, автентифікації, захисту мережевого трафіку та моніторингу з використанням програмної платформи Asterisk. Запропоновані підходи враховують характерні особливості корпоративного середовища та сучасні загрози інформаційній безпеці.

У першому розділі виконано глибокий аналіз теоретичних засад функціонування IP-телефонії, її архітектури, протоколів та основних апаратних і програмних компонентів. Проведено огляд сучасних механізмів забезпечення інформаційної безпеки, включаючи шифрування голосових даних, автентифікацію користувачів, засоби запобігання вторгненням та виявлення атак. Особливу увагу приділено типології атак на IP-телефонію, а саме DoS-атакам, перехопленню трафіку, підробці ідентифікаторів (spoofing) та підбору паролів (brute-force), які найчастіше зустрічаються у корпоративному середовищі.

У другому розділі систематизовано ризики та вразливості, що впливають на безпеку IP-телефонії. Обґрунтовано необхідність впровадження багаторівневого захисту з використанням таких технологій, як SIP-шифрування через TLS, захист медіа-трафіку за допомогою SRTP**,** використання міжмережевого екрана iptables для фільтрації трафіку та захисту від DoS-атак. Оцінено ефективність кожного із зазначених рішень, а також проаналізовано можливості систем активного реагування на загрози, зокрема Fail2Ban для захисту від атак перебору паролів на SSH та Asterisk, та обґрунтовано безпечну конфігурацію SSH.

У третьому розділі спроєктовано та реалізовано архітектуру підсистеми безпеки IP-телефонії на базі Asterisk. Визначено алгоритм впровадження механізмів безпеки, включаючи конфігурацію захищених SIP-з'єднань з використанням TLS, шифрування медіа-трафіку за допомогою SRTP, налаштування автентифікації клієнтів, реалізацію правил iptables для контролю доступу та захисту від DoS-атак, а також впровадження системи Fail2Ban для автоматичного виявлення та блокування

підозрілої активності. Запропоноване рішення дозволяє не лише захищати дані, що передаються, але й виявляти спроби несанкціонованого доступу на ранніх етапах.

Проведені заходи дозволили створити захищене серверне середовище IP-телефонії, яке демонструє високу ефективність у запобіганні більшості зловмисних дій, забезпечуючи стабільну роботу системи навіть в умовах підвищеного навантаження. Застосовані рішення знижують ризик сканування портів, запобігають брутфорс-атакам, обмежують можливості зловмисників у випадку компрометації та забезпечують механізми виявлення та реагування на спроби несанкціонованого доступу.

Набула подальшого розвитку інформаційна технологія захисту IP-телефонії на основі гнучкої програмної платформи Asterisk із інтеграцією протоколів TLS, SRTP та засобів активного реагування, таких як iptables та Fail2Ban**.** Запропонована архітектура орієнтована на корпоративні мережі, для яких важливо отримати надійний рівень безпеки без значних витрат на комерційні рішення.

Впровадження результатів роботи дозволяє підприємствам ефективно захистити комунікаційну інфраструктуру, підвищити стійкість до кібератак, забезпечити конфіденційність, цілісність та доступність голосового трафіку, що циркулює через IP-телефонію. Крім того, система забезпечує можливість моніторингу та аналізу подій безпеки, що сприяє своєчасному реагуванню на потенційні інциденти.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. – Hoboken : Pearson, 2020. 768 p.
2. Kumar P., Singh R. P. Network Security and Cryptography. Boca Raton : CRC Press, 2020. 300 p.
3. Bhaskar K. Network Security and Intrusion Detection Systems, 2023. 280 p.
4. Zetter J. A., L. A. Sayer. Securing the Internet of Things. Boca Raton : CRC Press, 2019. – 350 p.
5. Безпека інформаційних систем. URL : http://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem (дата звернення 23.05.2025)
6. Коваленко І. П., Кравченко С. В. Шляхи підвищення рівня захисту VoIP-систем на базі Asterisk. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. № 1(37). с. 87-94.
7. Смирнов В. Створення корпоративної voip-мережі із застосуванням софтфонів. URL : https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/25_MEICS-2023.pdf (дата звернення 23.05.2025)
8. Возможности Asterisk. URL: https://itua.com.ua/ru/318-2-ru(дата звернення 23.05.2025)
9. Волох В. Д., Ковальов О.П. Мережеві технології та безпека мереж. 2022. 250 с.
10. Що таке IP-телефонія і як це працює. URL: https://itel.ua/articles/shho-takeiptelefonijaijakcepracjuye?srsltid=AfmBOop49KdBR6gBldR868WSgZ5_Bcq7nj4odl1xtfj4XyITlugXgLQl (дата звернення 23.05.2025)
11. Лисенко А.О. Особливості впровадження системи забезпечення безпеки IP-телефонії. *Вісник Національного технічного університету України "КПІ". Серія "Інформатика, управління та обчислювальна техніка".* 2020. с. 75-81.
12. VoIP Steganography and Its Detection - A Survey. arXiv preprint. URL: https://arxiv.org/abs/1203.4374 (дата звернення: 24.05.2025).

13. Дзівак О.А. Модель забезпечення безпеки в IP-телефонії на прикладі Site-to-Site VPN. *Інтелектуальні комп'ютерні системи та мережі*: Матеріали IV науково-практичної конференції молодих вчених і студентів. 2021 р. Тернопіль. с. 6.

14. Дзівак О.А. Порівняльний аналіз протоколів для побудови мереж IP-телефонії. *Інтелектуальні комп'ютерні системи та мережі*: Матеріали V науково-практичної конференції молодих вчених і студентів. 2021 р. Тернопіль. с. 22

15. Іванов Д.В. Застосування віртуальних приватних мереж для захисту VoIP-трафіку в корпоративній мережі. 2021. с. 98-103

16. Securing Voice Over IP Networks. IEEE Computer Security and Privacy. URL: https://www.nist.gov/publications/securing-voice-over-ip-networks (дата звернення: 24.05.2025).

17. IP телефонія: що це, та як вона відрізняється від звичайної телефонії? URL:https://blog.globalbilgi.com.ua/ip-telefoniia-shcho-tse-ta-vidminnosti-vid-zvychainoi-telefonii/ (дата звернення: 24.05.2025).

18. Harris L. Practical VoIP Security. New York : Springer, 2017. – 330 p.

19. The Development of a Secure Internet Protocol (IP) Network Based on Asterisk Private Branch Exchange (PBX). URL: https://www.mdpi.com/2076-3417/13/19/10712(дата звернення: 24.05.2025).

20. SIP security issues: The SIP authentication procedure and its processing load. URL:https://www.researchgate.net/publication/3282875_SIP_security_issues_The_SIP_authentication_procedure_and_its_processing_load (дата звернення: 24.05.2025).

21. Detection of Abnormal SIP Signaling Patterns: A Deep Learning Comparison. URL: https://www.mdpi.com/2073-431X/11/2/27(дата звернення: 24.05.2025).

22. An ontology description for SIP security flaws. URL: https://www.researchgate.net/publication/222546646_An_ontology_description_for_SIP_security_flaws (дата звернення: 25.05.2025).

23. Shaw C. Defending Your VoIP Network. –San Francisco : Pearson. 2016. 295 p.

24. Rogers R. Network Security and VoIP. London : Elsevier, 2017. 328 p.

25. How to Eliminate SIP Communications Vulnerabilities. URL: https://voximplant.com/blog/how-to-eliminate-sip-communications-vulnerabilities (дата звернення: 25.05.2025).

26. Asterisk Official Website. URL: https://www.asterisk.org/ (дата звернення: 25.05.2025).

27. Telework Security Basics. URL: https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics (дата звернення: 25.05.2025).

28. Поліщук О.Р. Архітектура безпечної IP-телефонії для віддалених працівників. 2023. с. 98-106.

29. Morgan B. Security Essentials for VoIP. 2015. – 298 p.

30. Коваленко В.М., Ткаченко О.М. Аналіз сучасних загроз безпеці IP-телефонії та методи їх нейтралізації. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: Технічні науки*. 2019. –№ 3(79). – с. 138-149.

31. Abusing SIP authentication. URL: https://www.researchgate.net/publication/4377144_Abusing_SIP_authentication (дата звернення: 26.05.2025).

32. Evans D. Fundamentals of VoIP Security. 2017. 400 p.

33. Roberts F. VoIP: Securing the Network. 2018. 285 p.

34. Андрущенко В.О. Впровадження системи виявлення вторгнень для забезпечення безпеки Asterisk-сервера. *Збірник наукових праць Національної академії Служби безпеки України*. 2025. с. 65-72.

35. Черненко С.Д. Аналіз методів протидії спаму по VoIP. *Інформаційні системи та технології*. 2020. с. 70-76.

36. Безпека ip-телефонії для бізнесу: методи забезпечення та загрози. URL: https://a1call.me/blog/uk/2024/10/23/2711/ (дата звернення: 26.05.2025).

37. Що таке DDoS-атака?. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack (дата звернення: 26.05.2025).

38. Основні протокол IP-телефонії. URL: https://blog.globalbilgi.com.ua/6-osnovnykh-protokoliv-ip-telefonii/ (дата звернення: 26.05.2025).

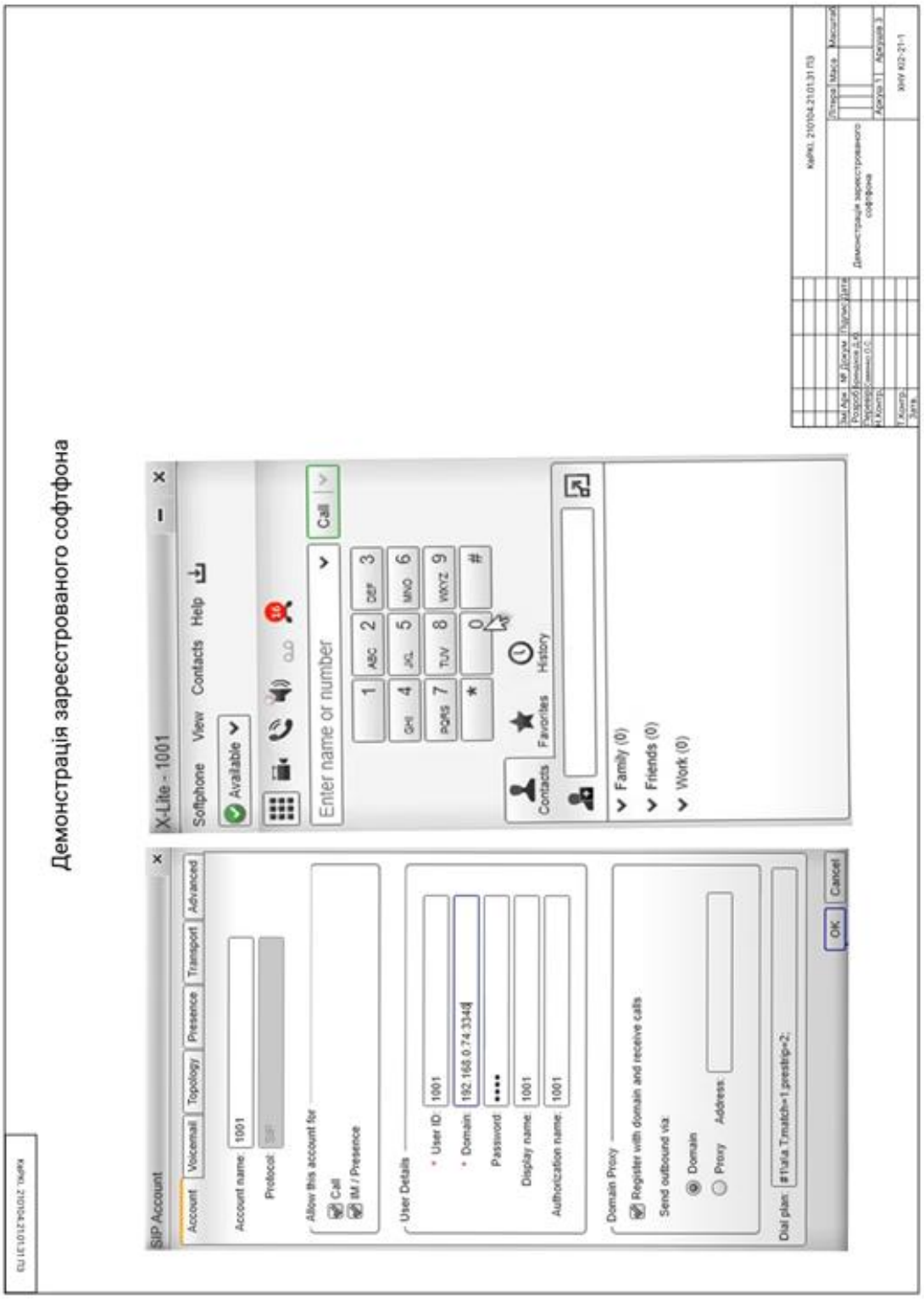
39. Baker L. Designing Secure VoIP Systems. 2017. 298 p.

40. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. URL: https://www.nist.gov/publications/guide-enterprise-telework-remote-access-and-bring-your-own-device-byod-security (дата звернення: 26.05.2025).

Додаток А

(обовя’язковий)

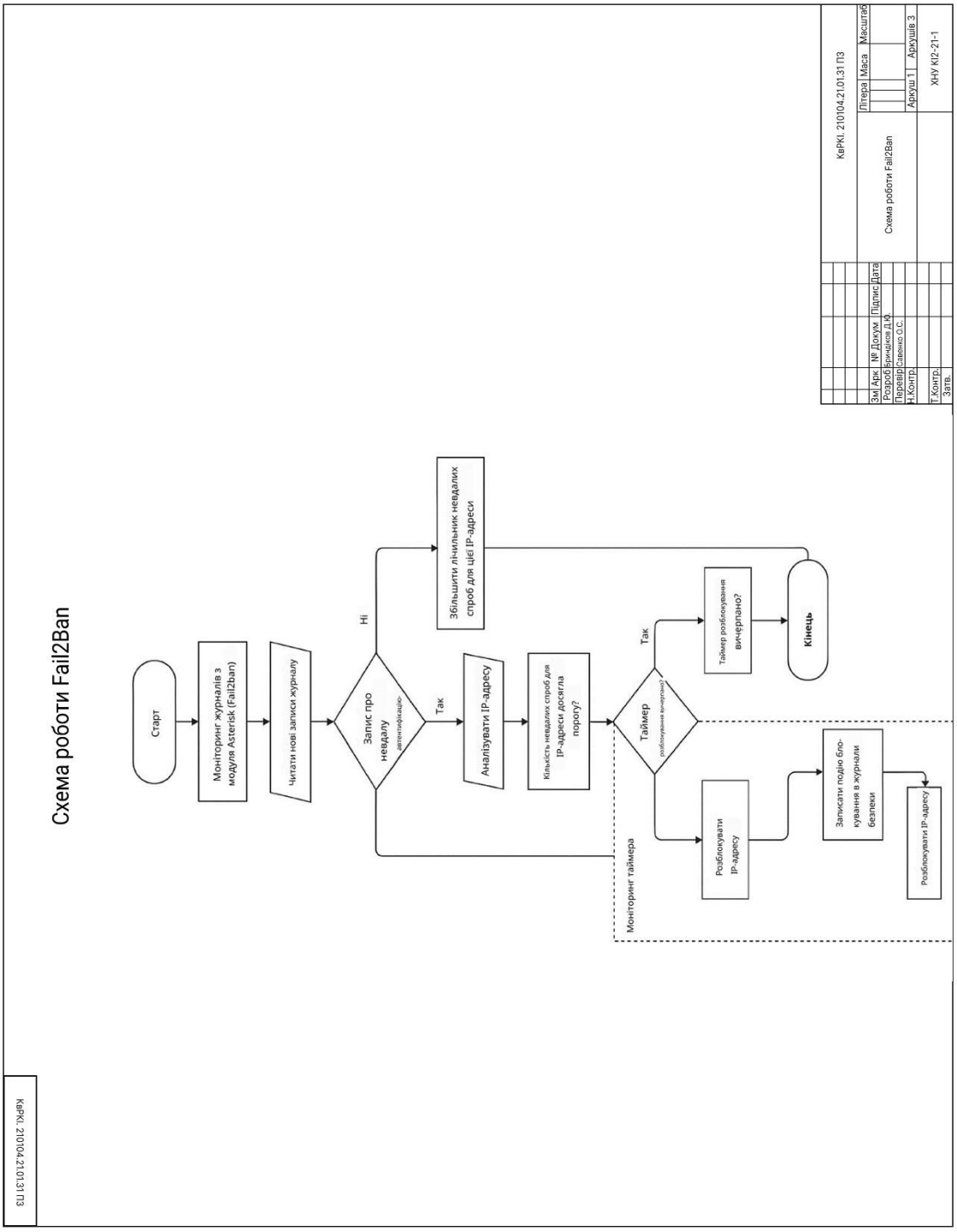
ДЕМОНСТРАЦІЯ ЗАРЕЄСТРОВАНОГО СОФТФОНА



Додаток Б

(обовя’язковий)

СХЕМА РОБОТИ FAIL2BAN



Додаток В

(обовя’язковий)

НАЛАШТУВАТИ FAIL2BAN ДЛЯ ЗАХИСТУ ASTERISK

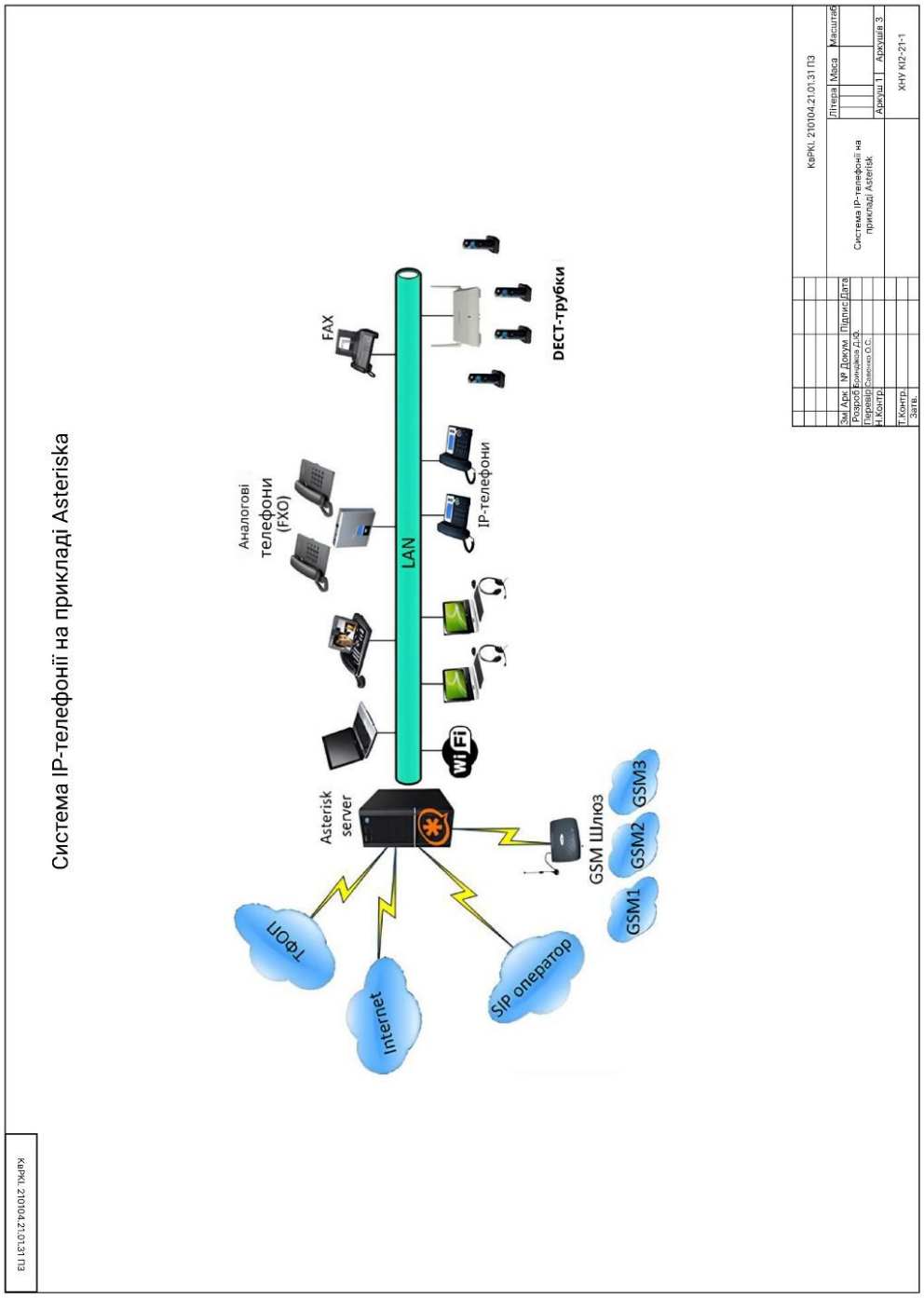
```
# Fail2Ban configuration file
[INCLUDES]
before = common.conf
[Definition]
failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*'
- Wrong password
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - No
matching peer found
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' -
Username/auth name mismatch
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - Device
does not match ACL
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - Peer is
not supposed to register
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - ACL error
(permit/deny)
NOTICE.* .*: Registration from '\".*\".*' failed for '<HOST>:.*' -
No matching peer found
NOTICE.* .*: Registration from '\".*\".*' failed for '<HOST>:.*' -
Wrong password
NOTICE.* <HOST> failed to authenticate as '.*'$
NOTICE.* .*: No registration for peer '.*' \(from <HOST>\)
NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)
NOTICE.* .*: Failed to authenticate user .*@<HOST>.*
NOTICE.* .*: <HOST> failed to authenticate as '.*'
NOTICE.* .*: <HOST> tried to authenticate with nonexistent user '.*'
VERBOSE.*SIP/<HOST>-.*Received incoming SIP connection from unknown
peer
ignoreregex = NOTICE.* .*: Registration from '.*' failed for
'<HOST>:.*' - Peer is not supposed to register
```

NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - ACL error (permit/deny)
NOTICE.* .*: Registration from '.*' failed for '<HOST>:.*' - Device does not match ACL
NOTICE.* .*: Registration from '\".*\".*' failed for '<HOST>:.*' - No matching peer found
NOTICE.* .*: Registration from '\".*\".*' failed for '<HOST>:.*' - Wrong password
NOTICE.* <HOST> failed to authenticate as '.*'$
NOTICE.* .*: No registration for peer '.*' \(from <HOST>\)
NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)
NOTICE.* .*: Failed to authenticate user .*@<HOST>.*
NOTICE.* .*: <HOST> failed to authenticate as '.*'
NOTICE.* .*: <HOST> tried to authenticate with nonexistent user '.*'
VERBOSE.*SIP/<HOST>-.*Received incoming SIP connection from unknown peer

Додаток Г

(обовя’язковий)

СИСТЕМА IP-ТЕЛЕФОНІЇ НА ПРИКЛАДІ ASTERISK



Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Даниїл БРИНДІКОВ

Співавтор:

Назва: БРИНДІКОВ_Підсистема забезпечення безпеки IP -телефонії в корпоративній мережі

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:13.4%

Коефіцієнт подібності 2:6.4%

Мікропробіли: 14

Заміна букв: 6

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-12 22:14:48.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-13 Доцент Андрій Нічепорук

Дата експерт

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 2.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 13%**

	Document		Sum coincidence on the DB	
ID: 245509 Title: БКР Підсистема забезпечення безпеки IP -телефонії в корпоративній мережі Added in a DB: 2025-06-13 Authors: Даниїл БРИНДІКОВ Heads: Світлана САЧЕНКО Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	95362	739	2961 (3%)	24 (3%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Бриндіков Даниїл Юрійович

Тема: Підсистема забезпечення безпеки IP-телефонії в корпоративній мережі

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 58

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є підсистема забезпечення безпеки IP-телефонії в корпоративній мережі.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено дослідження предметної області, пов'язаної з підсистемами забезпечення безпеки IP-телефонії в корпоративній мережі. Визначено мету і задачі дослідження.

У другому розділі кваліфікаційної роботи виконано моделювання та проєктування підсистеми забезпечення безпеки IP-телефонії в корпоративній мережі. Зокрема, сформовано архітектуру системи, обрано та обґрунтовано компоненти IP-телефонії, розроблено алгоритм збору, обробки та передачі даних, а також спроєктовано базову схему взаємодії пристрою з сервером. Створено блок-схему алгоритму функціонування системи, описано логіку обміну даними та структуру пакету даних для передачі.

У третьому розділі кваліфікаційної роботи виконано апаратну реалізацію системи, а саме: налаштування та конфігурування мережевого обладнання, що забезпечує функціонування IP-телефонії, а також впровадження програмних та апаратних засобів для підвищення рівня її безпеки. Зокрема, було розгорнуто

виділений сервер для хостингу АТС Asterisk, реалізовано міжмережеве екранування для фільтрації небажаного трафіку та налаштовано VPN-тунелі для захищеного обміну даними між віддаленими користувачами та корпоративною мережею. Крім того, проведено тестування функціональності та ефективності впроваджених рішень для підтвердження їхньої відповідності вимогам щодо надійності та безпеки системи.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: недостатня увага моделюванню схеми побудови IP-телефонії.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: не має

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Проворська Наталія Іванівна, доцент кафедри ІПЗ, к. пед. наук

"__"_____2025 р. _____(підпис)

Завідувачу кафедри КІІС

д-р. філософії, доц. Ользі ПАВЛОВІЙ

Даниїла Бриндікова

ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно зяким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному депозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

16.06 2025року

Бриндіков

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Підсистема забезпечення безпеки IP-телефонії в корпоративній мережі

Автор: Даниїл БРИНДІКОВ

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Світлана САЧЕНКО, к.е.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення наведено у розділах, присвячених аналізу існуючих аналогів і прототипів, які не містять опису власного дослідження та не пов'язані з результатами роботи;
2) усі запозичення є фрагментарними або супроводжуються належним чином оформленими посиланнями;
3) деякі виявлені збіги становлять загальновживані фрази чи вирази, що підтверджується посиланням системи на відповідність одній фразі з 10–40 джерел;
4) в окремих випадках система фіксує як запозичення послідовності чотиризначних двійкових кодів, які є типовими вхідними даними до великої кількості задач і не можуть вважатися об'єктом авторського права чи його порушенням;
5) усі виявлені системою ознаки зміни тексту стосуються лише поєднання латинських символів з україномовними скороченнями індексів у формулах, що не є зміною змісту тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 13.37% і адресується до 401 першоджерела; та системою Anti-Plagiarism складає 13.4%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Світлана САЧЕНКО

Гарант ОП _____ Андрій Нічепорук

Завідувач кафедри КІС _____ Ольга ПАВЛОВА